RESTRICTED 2

Service Organization Control 2 Type 2 Report

Description of Nexthink SA’s Experience system relevant to Security and Availability

For the period 15 December 2021 to 15 June 2022 with the Independent Services Auditor’s Assurance Report including Tests Performed and Results Thereof

08 November 2022

Table of Contents

1. Nexthink's Management Assertion

8th November 2022

We have prepared the accompanying Nexthink Experience (Description) of Nexthink (Service Organization) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria). The Description is intended to provide report users with information about the Nexthink Experience (System) that may be useful when assessing the risks arising from interactions with the System throughout the period 15th December 2021 to 15th June 2022, 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 for security and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Nexthink uses AWS and Azure for providing Infrastructure as a Service. The Description includes only the controls of Nexthink and excludes controls of AWS and Azure. The Description also indicates that certain trust services criteria specified therein can be met only if AWS and Azure's controls assumed in the design of Nexthink's controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of AWS and Azure.

The Description also indicates that certain trust services criteria specified in the Description can be met only if complementary user entity controls assumed in the design of Nexthink's controls are suitably designed and operating effectively, along with related controls at the Service Organization. The Description does not extend to controls of 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 15th December 2021 to 15th June 2022 in accordance with the Description Criteria.

b. The controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated as described and if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of Nexthink's controls throughout the period 15th December 2021 to 15th June 2022.

c. Except for the matters described in the following paragraphs, the Nexthink controls stated in the Description operated effectively throughout the period 15th December

2021 to 15th June 2022 to achieve the service commitments and system requirements based on the applicable trust services criteria, if user entities applied the complementary user entity controls and the subservice organizations applied the controls assumed in the design of Nexthink's controls throughout the period 15th December 2021 to 15th June 2022.

The management acknowledges the auditor's modified opinion based on the matters stated below:

- No comprehensive evidence was available for determining whether test objectives of the current disaster recovery plans were defined and that end-to-end tests were performed to validate the full scope of recovery activities. As a result of, the control was not operating effectively to achieve Trust Service Criteria A1.3, "*The entity tests recovery plan procedures supporting system recovery to meet its objectives*" and CC7.5 "*The entity identifies, develops, and implements activities to recover from identified security incidents.*"
- HR background screening reports are deleted after six months, and background screening was not requested for one sample. As a result of the mentioned scope limitation and noted exception for one selected sample, sufficient evidence could not be provided to determine the control was operating effectively to achieve Trust Service Criteria CC1.4 "*The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives*."
- Evidence was not available for the remediation of 3 out of 12 selected vulnerabilities, because of the limited retention time of the tool. In addition, the identified vulnerability of one sample was not resolved within the timeframe. As a result of the mentioned scope limitation, sufficient evidence could not be obtained to determine the control was operating effectively to achieve Trust Service Criteria 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.*"
- 5 out of 5 cloud changes did not adhere to the change process. As a result thereof, the control was not operating effectively to achieve Trust Service Criteria CC8.1 "*The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives*."

Our responses to the deviations identified are contained in Section V of the report.

Pedro Bados

Pedro Bados

CEO

Vedant Sampath

Vedant
Sampath

CTO

2. Independent service auditor's report

To the Management of Nexthink SA (Nexthink)

Scope

We have examined Nexthink's accompanying Description of the System of its Nexthink Experience system for offering a digital employee experience management platform throughout the period 15th December 2021 to 15th June 2022 (Description) in accordance with the criteria for a description of a service organization's system set forth in the Description Criteria DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (Description Criteria) and the suitability of the design and operating effectiveness of controls included in the Description throughout the period 15th December 2021 to 15th June 2022 to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services criteria for security and availability set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria).

Nexthink uses Amazon Web Services (AWS) and Microsoft Azure (Azure) as subservice organizations to provide Infrastructure as a service. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nexthink, to achieve Nexthink's service commitments and system requirements based on the applicable trust services criteria. The description presents Nexthink's system, its controls, and the types of complementary subservice organization controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS and Azure. Our examination did not extend to the services provided by AWS and Azure and we have not evaluated whether the controls management assumes have been implemented at AWS and Azure or whether such controls were suitably designed and operating effectively throughout the period 15th December 2021 to 15th June 2022.

The Description also indicates that Nexthink's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Nexthink's controls are suitably designed and operating effectively, along with related controls at the service organization. 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.

The information in the accompanying Section V: Other Information is presented by management of Nexthink to provide additional information and is not part of Nexthink's Description. Such information has not been subjected to the procedures applied in our examination and, accordingly, we express no opinion on it.

Nexthink's responsibilities
Nexthink 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 the service commitments and system requirements were achieved. Nexthink has provided the accompanying assertion titled Nexthink's Management Assertion (Assertion) about the presentation of the Description based on the Description Criteria and suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria. Nexthink is responsible for (1) preparing the Description and Assertion; (2) the completeness, accuracy, and method of presentation of the Description and Assertion; (3) providing the services covered by the Description; (4) identifying the risks that would threaten the achievement of the service organization's service commitments and system requirements; and (5) designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve its service commitments and system requirements.

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

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA") and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the Description is presented in accordance with the Description Criteria, and (2) the controls described therein are suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements would be achieved based on the applicable trust services criteria. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence we have obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

Our Independence and quality control

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

The firm applies International Standard on Quality Control 1 and accordingly maintains a comprehensive system of quality control including documented policies and procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent limitations

The Description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to its own particular needs.

Because of their nature, controls at a service organization may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls based on the applicable trust services criteria is subject to the risk that the system may change or that controls at a service organization may become ineffective.

Description of tests of controls

The specific controls we tested and the nature, timing, and results of those tests are listed in the accompanying Description of Trust Service Criteria, Controls, Tests and Results of Tests (Description of Tests and Results).

Basis for qualified opinion

Nexthink states in its Description that Test strategies exist to validate, adapt and improve current disaster recovery plans. However, as noted in the Description of Trust Service Criteria, Controls, Tests and Results of Tests, EY noted that no comprehensive evidence was available for determining whether test objectives were defined and that end-to-end tests were performed to validate the full scope of recovery activities.

As a result of, the control was not operating effectively to achieve Trust Service Criteria A1.3, "*The entity tests recovery plan procedures supporting system recovery to meet its objectives*" and CC7.5 "*The entity identifies, develops, and implements activities to recover from identified security incidents.*"

Nexthink states in its Description that Individuals offered a position at Nexthink are subject to background screening. However, as noted in the Description of Trust Service Criteria, Controls, Tests and Results of Tests, EY noted that evidence was not available for 3 out of 12 samples, because the background screening reports are deleted after 6 months. In addition, the background screening was not requested for one sample.

As a result of the mentioned scope limitation and exception for one selected, sufficient evidence could not be obtained to determine the control was operating effectively to achieve Trust Service Criteria CC1.4 "*The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives*."

Nexthink states in its Description that security vulnerabilities are remediated based on their criticality and impact with a defined SLA. However, as noted in the Description of Trust Service Criteria, Controls, Tests and Results of Tests, EY noted that evidence was not available for 3 out of 12 samples, because of the tool's limited retention time. In addition, the identified vulnerability of one sample was not resolved within the timeframe.

As a result of the mentioned scope limitation, sufficient evidence could not be obtained to determine the control was operating effectively to achieve Trust Service Criteria 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.*"

Nexthink states in its Description that Nexthink maintains a secure software development process, coding standards, and release strategy. However, as noted in the Description of Trust Service Criteria, Controls, Tests and Results of Tests, EY noted that 5 out of 5 cloud changes did not adhere to the change process.
As a result of, the control was not operating effectively to achieve Trust Service Criteria CC8.1 "*The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives*."

In our opinion, except for the matters referenced in the preceding paragraphs, in all material respects:

a. the Description presents the Nexthink Experience system that was designed and implemented throughout the period 15th December 2021 to 15th June 2022 in accordance with the Description Criteria.

b. the controls stated in the Description were suitably designed to provide reasonable assurance that the service commitments and system requirements would be achieved based on the applicable trust services criteria if the controls operated effectively and if the subservice organizations and user entities applied the controls assumed in the design of Nexthink's controls throughout the period 15th December 2021 to 15th June 2022.

c. the controls stated in the Description operated effectively to provide reasonable assurance that the service commitments and system requirements were achieved based on the applicable trust services criteria throughout the period 15th December 2021 to 15th June 2022, if the subservice organization and user entity controls assumed in the design of Nexthink's controls operated effectively throughout the period 15th December 2021 to 15th June 2022.

Restricted use

This report, including the description of tests of controls and results thereof in the Description of Tests and Results, is intended solely for the information and use of Nexthink, user entities of Nexthink's Nexthink Experience system during some or all of the period 15th December 2021 to 15th June 2022 and prospective user entities, independent auditors and practitioners providing services to such user entities who have sufficient knowledge and understanding of the following:

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

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

Ernst & Young Ltd

Markus T. Schweizer
Partner, licensed audit expert

Pascal Winkler
Director Attestation & Certification

3. Description of the System

3.1 Company background/ Intro

Nexthink is a leader in providing end-user digital experience management solutions. IT teams often do not have visibility into how employees consume services, or the impact of those services on their productivity and engagement. Nexthink Experience offers a digital employee experience management platform to help IT teams bridge this gap and continuously optimize the digital experience for employees. Nexthink's solutions combine real-time endpoint analytics and end-user feedback, through unique analytics and visualizations, to provide new insight and enable IT to be more proactive, reduce costs and enhance end-user productivity. Nexthink helps the end users, and in turn the organizations, to be safer, more productive, and more efficient by reducing IT flaws and errors. Nexthink Experience helps to alleviate employee frustration by eliminating IT-bottlenecks and allowing the helpdesk to identify problems earlier and pro-actively even before they occur.

Dual headquartered in Lausanne, Switzerland, and Boston, Massachusetts, Nexthink has 9 offices worldwide. Nexthink was founded in 2004 and has now more than 700 employees and continues to grow rapidly. Nexthink is helping more than 12 million employees across 1,000 customers, from the transport or healthcare industry, insurance companies, banks, luxe or retails sector.

3.2 Types of services provided

The scope of this report is the solution Nexthink Experience (cloud-based digital employee experience management platform) including all product components as well as the services used to deliver this solution. Also, in scope are Nexthink departments and corporate functions including product management, engineering, technical services, finance, HR, IT, legal, sales operations and security. This scope is a subset of the International Standard Organization (ISO) 27001:2013, 27017:2019 and 27018:2015 Information Security Management System (ISMS) and ISO 27701:2019 Privacy Information Management (PIMS) scope.

Nexthink solution comprises of the following components:

- Nexthink Analyze

Grants access to dashboards (including Experience Optimization), investigations, metrics, services, scores, categories, etc. to help an organization measure the digital experience of employees.

- Nexthink Web & Cloud

Grants access to analytics related to intranet and extranet HTTP and HTTPS web requests (now included by default in Nexthink Analyze for new contracts).

- Nexthink Act

Offers an organization a way to remotely act on the devices of the employees for automated or assisted servicing.

- Nexthink Engage

Gives an organization the means to reach out to their employees, gather their feedback regarding IT or other subjects, and notify them of relevant issues.

- Nexthink Integrate

Enables the product API and access to continuously improved integration samples, reports, etc.

3.3 Principal Service Commitments and System Requirements

Nexthink designs its processes and procedures related to its solution to meet the objectives of its services. These objectives are based on the service commitments that Nexthink makes to user entities, and the operational and compliance requirements that Nexthink has established for the services.

Service commitments to user entities are documented and communicated in Service Level Agreements (SLA) and other contractual agreements, as well as in the description of the service offering provided to its customers. Service commitments are duly documented in the Master Cloud Service Agreement and supporting security policies. They include, but are not limited to, the following:

Nexthink Experience commitments (as mentioned below) are:

- Perform at least yearly external independent audits.
- Ensure that access to production is restricted and follows a formal approval process.
- Use security mechanisms to protect customer data in motion and at rest.
- Maintain a formal Security Incident Response Plan including required tools and platforms to detect and trace security events.
- Maintain Business Continuity and Disaster Recovery plans to help ensure the availability of service and critical operations in case of a major disaster.
- Ensure production uptime is in accordance with defined SLA.
- Follow adequate change management and users’ incident management to ensure that the functionalities of the solution run as expected by the established design and that identified bugs are corrected in a timely and appropriate manner.

3.4 Underlying architecture

- Nexthink V6aaS is built on a software stack comprised of multiple tiers relying on a set of technologies, based on the features as mentioned below:
- For investigation and dedicated views of data: Nginx, Jetty, PostgreSQL and a proprietary in-memory C++ database and application server.
- For the web-based dashboarding and administrative features: Nginx, Jetty and PostgreSQL.

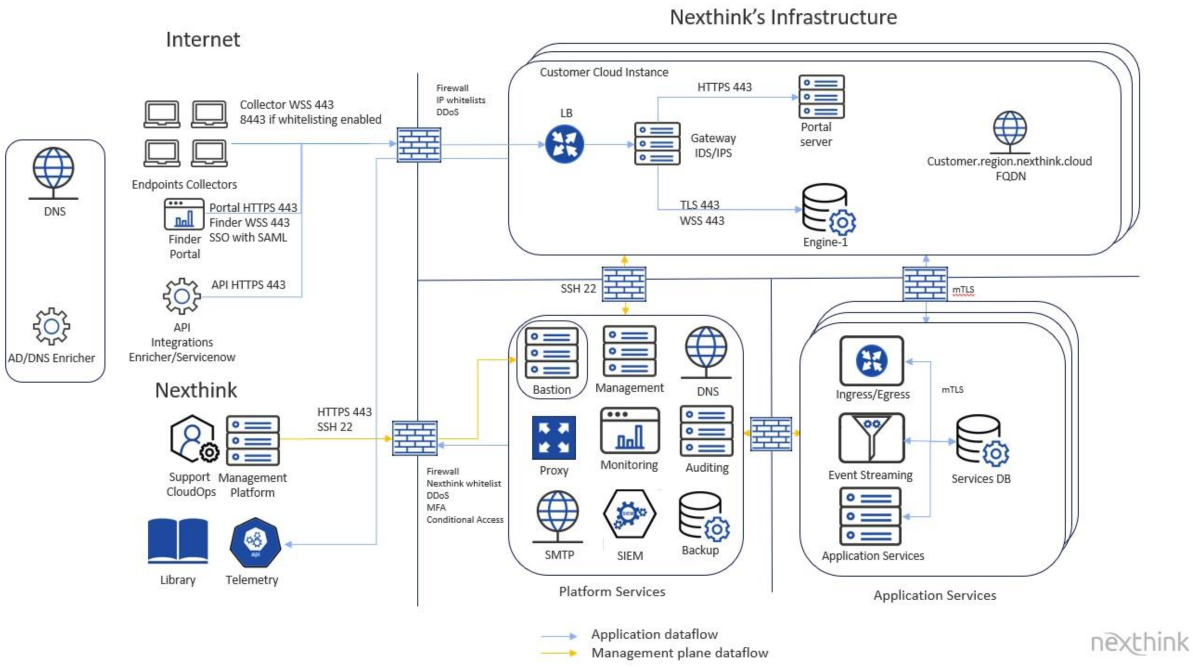
The reporting (computation) stack is comprised of In-House in-memory database and application server.

Nexthink NEXaaS is built on a software stack comprised of 3 main tiers:

- **Data platform tier**: Comprised of a data pipeline, with microservices technologies for ingestion, aggregation, tagging, alerting, identification and storage of events and inventory data. With Kubernetes, Kafka, PostgreSQL and ClickHouse as main infrastructure components.
- **Feature tier**: Comprised of Java, Scala, NodeJS, and Python microservices; Deployed in Kubernetes and using Kafka, PostgreSQL and ClickHouse.
- **Front-end tier**: Comprised of React.js, Nginx, GraphQL, Node.js and Java and Scala microservices. Deployed in Kubernetes, accessible through API gateway and K8S ingress gateways.

Nexthink has documented procedures on how to instantiate both SaaS platforms. These procedures include getting quality assurance (QA) approved release source code from Bitbucket and using Jenkins pipelines creating the corresponding binaries or docker images into Artifactory, moving these container images to corresponding container registries (AWS ECR for both the V6aaS and NEXaaS), installing and configuring applications and the databases, modifying configuration properties, and modifying domain name server (DNS) settings. For V6aaS part of the build process, we create virtual disk images for AWS.

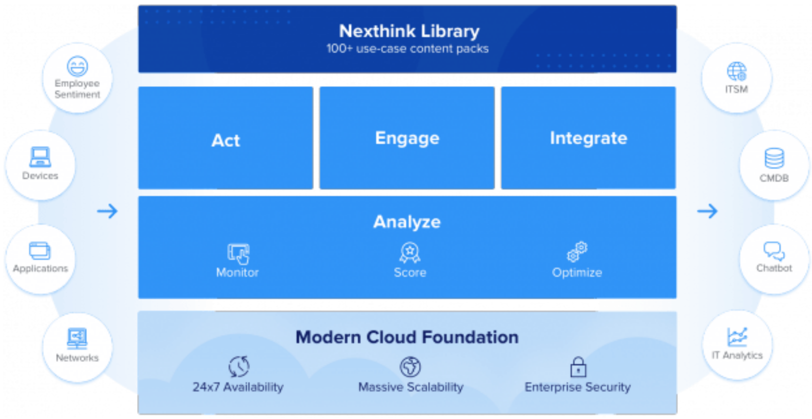
The architecture of Nexthink Experience has been designed to simplify operations, ensure scaling, and allow rapid deployment. Security principles and requirements are embedded by design in the architecture.



Nexthink Experience infrastructure diagram

The Nexthink platform is composed of the following elements:

- The Collector captures information from the devices of employees.
- A modern cloud foundation aggregates Collector data and provides real-time IT analytics.
- The Finder is a rich client application for searching and analyzing data stored in the cloud foundation.
- The Portal provides dashboarding (including Experience Optimization), reporting, and long-term trending for analytics.
- The Nexthink Library is a cloud content packs and integrations database with ready-made content for both the Portal and the Finder that addresses a variety of use cases.



Nexthink Experience component diagram

3.5 Infrastructure components description

Nexthink relies on Azure and AWS as IaaS providers for its SaaS platform. Nexthink leverages the use of public cloud solutions, Azure and AWS, as an underlying technology to provide scalable and flexible infrastructure that is capable to offer services based on latest technologies, react to market trends, and deploy services faster than traditional in-house data center management. Nexthink leverages multiple Azure and AWS regions. With both providers, it uses multiple availability zones within each region for redundancy and disaster recovery purposes to help ensure the availability of the platform.

Nexthink does not own or maintain any of the hardware located in the Azure or AWS datacenters and operates under a shared security responsibility model, where Azure or AWS is responsible for the security of the underlying cloud infrastructure (e.g., physical infrastructure, geographical regions, availability zones, edge locations, operating, managing, and controlling the components from the host operating system, virtualization layer and storage). Nexthink is responsible for securing the SaaS platform deployed in Azure and AWS (e.g., customer data, applications, identity and access management, databases, operating system and network firewall configuration, network traffic, server-side encryption) and the operation of the IaaS as defined in the providers' CUEC.

The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below.

Primary infrastructure			
Production **Application**	**Business function description**	**Technology**	**Physical Location**
V6aaS	Nexthink V6, a single-tenant application that provides analytical insights on employee experience, application experience and allow to execute remote actions, campaigns on devices. Composed of Finder, a fat client to create investigations, get views on data (user view, device view) and web-based application.	RPM, CentOS VHD images, Jetty, Nginx, Consul, Java virtual machine, PostgreSQL	Multiple AWS regions chosen by customer Set of Azure regions (one by continent) for API entry points and DNS
NEXaaS	Nexthink Experience, a web-based single and multi-tenant application that provides analytical insights on employee experience, application experience and allow to execute remote actions, campaigns on devices.	Docker, Kubernetes, Helm, Java virtual machine, Istio, PostgreSQL, ClickHouse, Kafka	Multiple AWS regions chosen by customer

Azure VM	Virtualized network and processing infrastructure to host Nexthink V6aaS entry point.	N/A	Multiple Azure regions chosen by customer
Azure Key Vault	A key management component to host secrets used by Nexthink V6aaS entry point.	N/A	Multiple Azure regions (one per continent)
AWS MSK	Kafka cluster as streaming platform for Nexthink NEXaaS data pipeline.	N/A	Multiple AWS regions
AWS SecretsManager	A secret management component to host secrets used by Nexthink NEXaaS.	N/A	
AWS IAM	Identity and access management component to provide cloud access control.	N/A	
AWS ECR	Registry of Nexthink container images that are used for Nexthink NEXaaS.	N/A	
AWS EC2	Virtualized network and processing infrastructure to host Nexthink V6aaS and NEXaaS ClickHouse clusters.	N/A	
AWS RDS	PostgreSQL cluster to host Nexthink NEXaaS inventory, content, configuration and access rights management data.	N/A	
AWS EKS	Kubernetes cluster running Nexthink NEXaaS microservices.	Amazon Linux 2	
AWS GuardDuty	Threat detection service	N/A	
AWS VPC	Virtual networking	N/A	

Primary infrastructure			
Production **Application**	**Business function description**	**Technology**	**Physical Location**
AWS API Gateway	API gateway for public and internal APIs of NEXaaS.	N/A	Multiple AWS regions
AWS DynamoDB	Key-value database to store and retrieve routing information for lambda authorizer for API gateway used by NEXaaS.	N/A	
AWS SES	Email service used by NEXaaS to send emails in context of alerts configured by end-users.	N/A	
AWS Route 53 (DNS)	DNS server that hosts API gateway public names.	N/A	
AWS EC2 ELB	Elastic load balancer used by NEXaaS.	N/A	
AWS Lambda	Lambda authorizer of API gateway that validates the access tokens for NEXaaS.	N/A	

3.6 Boundaries of the system

The scope is described in the chapter “Type of services provided”. Any other environment not described in this report is outside the boundaries. Notably, this report does not apply to user entities running and hosting the application and underlying production database on their own IaaS subscriptions and on-premises installation.

Professional services and managed services are out of scope.

Nexthink uses subservice organizations to provide them with the required technologies (notably IaaS resources and software tools) and support services. Complementary subservice organizations’ controls (detailed in the next section) that are suitably designed and operating effectively are necessary, along with controls at Nexthink, to achieve Nexthink’s service commitments and system requirements based on the applicable Trust Services Criteria. This report does not cover the services provided and controls performed by any subservice organizations and the related subservice organizations are fully responsible for the related controls’ appropriate design and operating effectiveness.

Moreover, complementary user entity controls (detailed later in the dedicated chapter) that are suitably designed and operating effectively are necessary, along with controls at Nexthink, to achieve Nexthink's service commitments and system requirements based on the applicable Trust Services Criteria. This report also does not cover the related controls performed by Nexthink's customers and customers are fully responsible for the related controls' appropriate design and operating effectiveness.

3.7 Subservice organizations carved out of the scope of the report

The Infrastructure as a Service providers, AWS and Azure that are used for hosting Nexthink cloud infrastructure were not included within the scope of this assessment (examination).

The following services were not included within the scope of this assessment:

Domain	Subservice name	Service provided / processes managed by the subservice organization
Infrastructure and related incident, change, operation, and monitoring management	Azure	Infrastructure as a Service
	AWS	
Communication, incident and change management	Zendesk	Product Support platform
Change management	Atlassian Jira /	Managed Services project management
Documentation	Confluence Cloud	Documentation and knowledge base platform
Identity and Access Management	Azure AD, Okta, Duo Security	Identity and Access Management platform
Information and Communication	SendSafely	Secure file-sharing service
Detection and management of security events	Mnemonic	Managed Detection and Response service

3.8 Data

Data, as defined by Nexthink, is constituted of the following:

- Inputs
  - “Nexthink Analytics” and “Nexthink Web & Cloud“:
    - Objects (represent real life items recognized by Nexthink)
    - Activities (represent actions performed by Objects)
    - Events (are warning or errors)
  - “Nexthink Act” event logs
  - “Nexthink Engage” responses
  - Support Telemetry
- Transactional data
- System files
- Outputs
  - reports generated (via Finder or Portal)
  - data queried by or pushed to the customers’ system (via API Integrations)

Nexthink does not process any information about the content of files, e-mail, websites, or any other content.

3.9 Supporting software, services, and tools

Nexthink relies on different software and services to deliver the cloud offering and the control environment. The table below illustrates this list:

Component	**Service**
Code and release management	Bitbucket, Jenkins and Artifactory
Third-party RPM packages and docker images repository, as build library	Artifactory, AWS Elastic Container Registry
Secure remote access to the production environment	Bastion, SSH, AWS Systems Manager (SSM) Session Manager
Corporate uptime monitoring and SLA reporting	Pingdom
Customer Support platform	Zendesk
Security and audit	AWS CloudTrail
Computing	Azure VM AWS EC2
Networking	AWS VPC

Container orchestration	AWS EKS
Databases	ClickHouse Kafka In-memory C++ database PostgreSQL AWS Aurora
Storage services	Azure blob storage AWS S3 AWS EBS
Production Monitoring	Grafana Azure LogAnalytics NewRelic AWS CloudWatch PagerDuty
DDoS protection	Cloudflare, AWS, and Azure
Endpoint Detection and Response (EDR)	Palo Alto Networks Cortex XDR Pro
Vulnerability management	Tenable Security Center
Identity and Access Management service	Okta AWS Identity and Access Management (IAM) AWS Single Sign-On (SSO) Azure Active Directory (AAD)
Log management and SIEM	Splunk Enterprise Security
Managed Detection and Response	Mnemonic
Risk and Vendor Management	Service Now Integrated Risk Management (IRM)

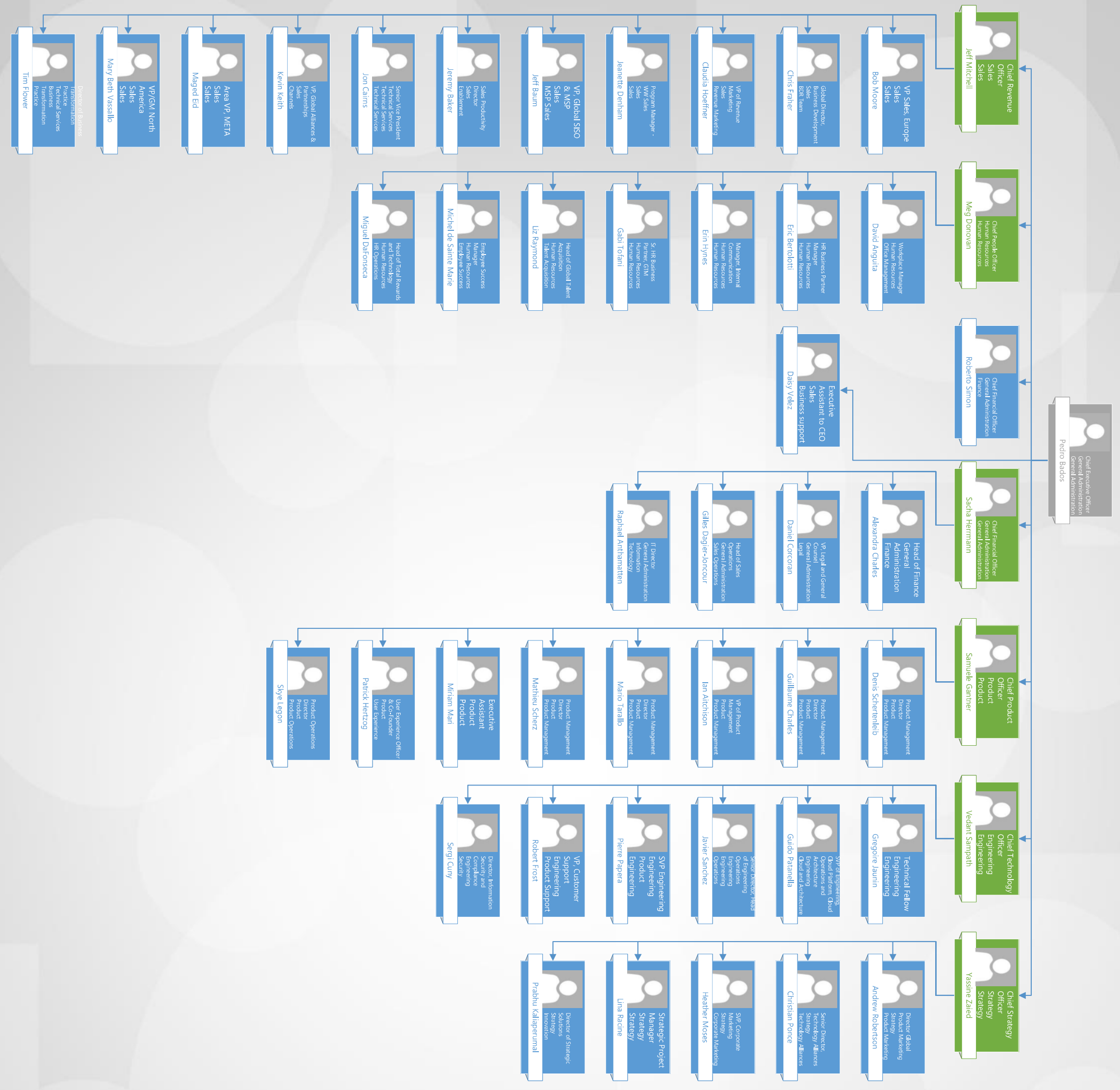
Team collaboration	Atlassian Jira and Confluence
Virtual Private Network (VPN)	OpenVPN, Zscaler
Multi-Factor Authentication (MFA)	Duo Security
Corporate Communication	Microsoft 365, Zoom
Customer Management	Salesforce
Talent performance	Lattice
Human Resources Information System (HRIS)	BambooHR
Applicant Tracking System	SmartRecruiters
Learning and development	Bridge App
Security awareness email campaigns	Knowbe4
Password Management	1Password
Corporate device management	JamF Pro, Intune, JumpCloud
Cloud security posture management	Fugue
Static Application Security Testing	SonarQube, PVS-Studio
Quality Assurance software	Testrail
Software Component Analysis and Dependency scanning	JFrog Xray, OWASP Dependency check, Snyk
Secret Management	AWS Security Token Service (STS) HashiCorp Vault
Infrastructure-as-Code (IaC)	HashiCorp Terraform
Configuration management	HashiCorp Ansible
Network Intrusion Detection System	Palo Alto Network Firewall, Cortex XDR Pro and XDR AWS GuardDuty

3.10 Organizational structure

Nexthink relies on the following teams to design, develop, operate and support Nexthink Experience cloud offering:

- **Board of Directors (BoD)**: Responsible for establishing and overseeing the company's strategy.
- **Senior Management (SM)**: Responsible for the execution of the strategy and oversees all the company operations. This team includes all C-levels and reports to the Board of directors.
- **Product Management (PM)**: Responsible for defining the product strategy, including, but not limited to, adding new features, documenting the product, collecting customer feedback and delivery training to customers.
- **Engineering (ENG)**: Comprised of multiple teams responsible from designing to supporting the cloud offering:
    - **Engineering**: Responsible for designing, developing, and delivering the Experience cloud offering.
    - **Cloud Operations (CloudOps)**: Responsible for operating the Experience cloud offering.
    - **Product Support**: Responsible for providing timely and effortless help that keeps customer's needs at the forefront of every interaction.
    - **Security and Compliance (SEC)**: Comprises of three teams responsible for overseeing Information Security aspect of the cloud offering including, application, cloud, corporate security, and compliance matters as described in the Security Governance policy and reports to the SM.
- **Information Technology (IT)**: Provide both infrastructure and support internally to the control environment, including, but not limited to, hardware, software maintenance and support.
- **Human Resources (HR)**: Comprise of the Talent Acquisition team, the Employee Success team, the HR Business Partners, the Office Management team, the HR Operations teams. They are responsible for onboarding, offboarding, training employees and performance management, including compensation and benefits.
- **Legal (LEG)**: Responsible for providing the legal review and support for all privacy and legal matters.

High level organizational Chart:



3.11 Governance and oversight

3.11.1 Board of Directors

A Shareholders' agreement outlines the roles, responsibilities, and authorities of the BoD (individually and collectively).

The Shareholders' agreement includes relevant information about the governance process, including information about membership, independence, committees / meetings, conflicts management, access to management and independent advice, continuous training, performance review.

The Shareholder agreement is frequently reviewed to ensure that it remains appropriate and that it addresses the concerns of the current environment.

The BoD is led by the yearly appointed chairman and oversees the company's strategy and organization, including, but not limited to financial control and planning.

3.11.2 The Audit Committee

The Audit Committee is responsible for, among other things:

- overseeing and monitoring the integrity of Nexthink's consolidated financial statements, the entity's compliance with legal and regulatory requirements as they relate to financial reporting or accounting matters, and the organization's internal accounting and financial controls.
- overseeing and monitoring Nexthink's independent auditor's qualifications, independence, and performance.
- providing the Board with the results of its monitoring and recommendations.
- providing the Board with additional information and materials as it deems necessary to make the Board aware of significant financial matters that require the attention of the Board; and overseeing the Nexthink's internal audit function.

The Audit Committee generally meets at least once a year and has discussions with both the external and internal auditors at each meeting.

Independent audits are conducted for information security and financial statements at least annually. Audit results and appropriate corrective measures are reviewed by the BoD.

3.11.3 Management Meeting

The management meeting, chaired by the CFO, is comprised of the SM and reports to the BoD. It has been delegated by the BoD the responsibility for managing Nexthink and its business on a daily basis.

Lines of authority and responsibility are clearly established throughout the organization under the SM.

3.11.4 Information Security Management System (ISMS) & Privacy Information Management System (PIMS) committee

This committee is led by the VP of Information Security and reports to the Management Team. SM represented by CFO and CTO reviews the development, implementation, and maintenance of ISMS & PIMS. This includes:

- Communication and training status
- Corrective and preventing controls validation
- Corrective and preventing controls follow-up
- Project follow-up
- Security Incident review since last meeting
- Internal Audit review since last meeting
- Non-conformities point follow-up

ISMS & PIMS committee is held twice a year to discuss each of these aspects.

3.11.5 IT / Security / Engineering Steering Committee

Steering Committee is led by the Director of Information Security and Compliance. This includes:

- Current project status
- New projects
- Overall status (Security and Compliance)

Steering committees are held quarterly to discuss each of these aspects.

3.11.6 Setting objectives with OKR

To support the principal objectives and service commitment, Nexthink relies on the Objectives & Key Results (OKRs) framework to define Company, Department and team objectives and key results.

- Company OKRs to drive the main goals annually
- Departmental OKRs quarterly with main initiatives in the quarter

OKR are reviewed quarterly and reported to SM.

3.12 People management

3.12.1 Hiring process

Managers within the respective functional groups of the organization determine the need for additional resources and submit formal job requisitions to SM for approval. Once approved, HR begins sourcing for the available position. HR screens potential candidates and send selected résumés to the respective hiring managers. The hiring managers review documentation, select candidates, and inform HR of individuals with whom they wish to schedule interviews. The relevant manager and HR conduct interviews and potential offers are submitted to the appropriate authority within the organization for approval.

Individuals offered a position at Nexthink are subject to background screening (as appropriate for each country with respect to local laws and regulations) prior to commencing employment. The background screening for employees includes substantiation of educational credentials and previous employment. Prospective employees complete an employment application and sign waivers to release information for the background screening. In addition, it is the policy of Nexthink to request employment references to determine whether the candidate is well-qualified and has the potential to be productive and successful during his or her tenure.

3.12.2 Onboarding process

Nexthink has developed a comprehensive set of programs to onboard new employees for employee onboarding:

- **The Buddy Program for newcomers** Every newcomer is provided with a “buddy” to support newcomers throughout their Nexthink journey. Buddy’s role is to welcome and introduce them to the teams, tutor them and help them master new functions (including shadowing), be a friendly and supportive ally, always be available and reduce onboarding responsibilities of the manager.

- **Welcome Sessions**: Through these sessions, newcomers are given the opportunity to meet the Top Management team so that they can discover more about the company, the mission, the core values, and each department. Additionally, field training is organized by the Sales Enablement team and is designated for Marketing, Sales, CSO and Strategy newcomers. It also includes Legal and SFDC trainings. R&D training is intended for Engineering and Product newcomers.
- **Learning Path in Nexthink Academy**: Newcomers are required to complete training module in the Academy which contains essential information about the company's' culture and values, product, customers, security awareness, legal awareness & GDPR overview, and corporate tools.

Nexthink provides mandatory Security and Privacy awareness training to its employees including information about, but not limited to, risk pertaining to our activities, monitoring and audit process, privacy requirements, roles and responsibilities, acceptable usage policy, confidentiality guidance, and incident response procedures.

The training must be completed within first three months of joining Nexthink (initial training) and annually (continuous training). Nexthink provides technical trainings to engineers aligned to the sensitivity of the data and systems they are required to perform their job duties which must be completed annually.

The training materials are reviewed on a yearly basis or upon changes.

3.12.3 Performance management

- HR Management and Reporting**:** Formal job descriptions including skills, responsibilities for different job positions are in place and agreed by employees.
- Employee Incentives and Rewards**:** Each year, Nexthink recognizes its 20 % highest performing and impactful employees. Out of them, Individual (I) - I1, I2, I3, Management (M) - M1 & M2 job levels get stock-options as a reward to recognize their hard work and commitment to Nexthink.
- **Employee Performance Review Process**: Assessment of the employees' performance based on adherence to "Core Values and Behaviors" is part of the employee performance review performed on a yearly basis.

3.13 Integrity and ethical values

At Nexthink, our core values (as listed below) are at the forefront of everything we do. They serve as the guiding principles behind every piece of code we write, digital transformation we plan, Nexthinker we hire, and meal we share:

- **Positive attitude**: Negativity gets you nowhere. We face challenges with a positive attitude.
- **Getting things done**: We are always looking for the fastest and smartest way to get the job done.
- **One team**: We are all in this together.

- **Continuous improvement**: Our desire to learn and improve never stops

The Nexthink Code of Conduct completes Nexthink's values and how to put these values into practice. Nexthink commitment to the principles of the Code determines the excellence of the people Nexthink can attract and retain, the leadership role of Nexthink's products in the marketplace, and the transformational value Nexthink brings to our customers.

Nexthink's staff acts with integrity in our work and our community.

- **Integrity**: The cornerstone of our Code of Conduct is the Nexthink commitment to integrity. We treat others with respect and operate with respect for the laws and the practices of our community. Operating with integrity runs through our core values and our internal mission statement, with focus on attitude that guide fair and open interactions, within a proactive and rewarding work environment.
- **Compliance with Law and Ethics**: Nexthink is committed to protect our company's reputation and legal standing by complying with all applicable laws. Nexthinkers are expected to be ethical and responsible when dealing with our company's finances, products, partnerships, and public image.
- **Commitment to Free and Fair Competition**: Nexthink is committed to a free and fair marketplace, and we support fair and effective competition. We refrain from any anticompetitive behavior and agreements of any kind in respect of price, markets, territories, and clients.
- **Anti-Corruption**: Nexthink prohibits bribery for the benefit of any external or internal party. We are careful not to offer favors to business partners to secure an order or to public officials to influence their actions. Nonetheless, we may engage in usual promotional and lead generation activities, as established under our policies.

Nexthink's staff protects the best interests of Nexthink with Integrity. We represent Nexthink to the world in a professional and positive manner and protect its assets and confidential information.

- **Representation of Nexthink**: We act professionally and appropriately at all times when representing Nexthink. We continuously work to gain the trust and respect of our customers and establish a trusted relationship with our business partners.
- **Protection of Nexthink Property**: All Nexthinkers treat our property (including intellectual property and company information such as trademarks, copyright, and others), whether material or intangible, with respect and care, protect it against loss and damage and use it solely for legitimate purposes.
- **Nexthink Confidential Information**: Nexthink does not allow access to confidential information or commercial secrets to unauthorized or external persons. Nexthink does not misuse such information for personal gain or for unauthorized third-party advantage. Information we acquire within the scope of our business activity is always used appropriately and to the extent permitted and commercially justified.

Nexthink's staff works together with integrity. We act professionally, maintain a safe and respectful workplace, and avoid conflicts. We also work collaboratively, including through open and clear communication.

- **Equal treatment**: Nexthink is committed to gender equality and equal treatment for people of different races, national or ethnic origins, religions, ages, sexual orientations, gender identities or expressions, veteran status, or backgrounds.
- **Professionalism**: All Nexthinkers must show integrity and professionalism in their roles as Nexthinkers. We treat each other with fairness and respect. We endeavor to create a working environment that is guided by personal responsibility and achievement.
- **Respect in the Workplace**: We respect our colleagues. We do not tolerate discriminatory behavior, harassment, bullying or victimization in any form, whether verbal, physical or visual.
- **Conflict of interest**: We expect Nexthinkers to avoid any personal, financial, or other interests that might negatively impact their capability to perform their job duties or create the appearance of impropriety in their professional role.
- **Collaboration**: Nexthinkers strive to be friendly and collaborative and not disrupt workplace or present obstacles to our colleagues' work. We have mutual respect for one another's privacy and personal dignity.
- **Communication**: Nexthink is open to communication via open dialogue with our colleagues, supervisors or team members using respectful and clear language We are transparent and positive in our interactions. With respect to our external-facing communication, we communicate in a direct, transparent, and non-misleading way.
- **Benefits**: Nexthinkers respects the boundaries of our employment benefits with respect to time off, facilities, subscriptions, or other benefits our company offers.

Nexthink has established an anti-Harassment policy to ensure a respectful Workplace along with a Global Anti-Bribery Policy to conduct all business in an honest and ethical manner.

A Whistleblower Policy is in place to provide guidance for reporting violations to the Code of Conduct or other policies. A dedicated team is responsible to investigate the reported violations.

3.14 Security Controls

Nexthink employees shall accept and apply the Nexthink policies, procedures and baselines that define how services should be delivered. These are located on the company documentation repositories and can be accessed by every Nexthink employee on a need-to-know basis.

We have described the main controls below.

3.14.1 Logical and Physical Access controls

Access to information assets to authorized users, infrastructure and software is based on the Access Control policy governed by the following principles:

- Least privilege principle
- Single sign-on
- Non-repudiation
- Multifactor authentication
- Protection of secret authentication information
- Segregation of duties

3.14.1.1 Authentication

Nexthink relies on Okta and Azure AD as Identity and Access providers for corporate systems, internal services, and applications. They are integrated with Okta through SSO to deliver authentication and authorization capabilities. Okta is integrated with multifactor authentication service of Duo Security. Nexthink provides support for federated Identities through SAML 2.0.

IT Infrastructure remote management is performed via SSH using key-based authentication. Password-based and weaker authentications are disabled by default.

Access to office network via Wi-Fi is authenticated using IEEE 802.1x Network Access Control (NAC). Authenticated users are assigned a Virtual Local Area Network (VLAN) based on their role.

3.14.1.2 Authorization

Access to information and IT system resources are granted on a “need to know” or “least privilege” basis and must be authorized by information asset owner. Access must be granted using Role based access controls (RBAC). Access to networks, systems, and applications is granted based of the principle of least privilege.

IT Team maintains a list of roles per job position to ensure systematic and efficient provisioning.

Nexthink is using IaC to define roles and accesses in the Engineering department. Reviews and approvals are only performed by authorized staff.

3.14.1.3 Account lifecycle:

Nexthink corporate accounts are managed throughout their entire lifecycle, following dedicated process. The source of truth for HR Employee information is the HRIS and is synchronized with the IT Support ticketing system.

- **Onboarding**: Nexthink new-hires on-boarding is coordinated between HR and IT to ensure appropriate access provisioning and system configurations are in place for each new hire. Access provisioning to new employees is directed by the HRIS which are integrated with IT systems.
- **Change of Role**: Access is modified for employees changing roles or requesting additional entitlements. Procedures are defined to ensure appropriate permissions are assigned upon role change.
- **Offboarding**: Access is revoked for employees changing roles or leaving the company. When the HR Operations team changes the termination date of an employee's contract, an offboarding ticket is automatically opened on the IT service desk, specifying the employee details and contract end date. The IT team then follows the procedures to offboard the employee.
- **Access reviews**: Access reviews are performed at regular intervals (at least yearly) and recertified at least once a year. Deviations are validated and corrected by systems owner.

3.14.1.4 Access to production environment

Nexthink applies tight access control to production environment. Authorized Nexthink employees can access the customer's production instance. Access to production data on AWS is managed through AWS SSO connected to Nexthink Okta IdP and based on role-based access control limited to authorized personnel. In addition, CloudTrail is enabled ensuring access to data is logged. Access to virtual machines is performed via SSH on top of AWS SSM.

Access to the platform and the customer data are authorized separately. Some employees have permanent access according to their role (e.g., CloudOps or Security).

To allow temporary access to the production environment for platform support or troubleshooting, Nexthink has implemented a procedure for engineers who do not have access to production to request a temporary access to specific resources in the AWS production environment.

3.14.1.5 Secret management

Nexthink securely manages credentials of service accounts, which includes IP allow-listing and temporary credentials using the AWS STS and HashiCorp Vault.

Nexthink Experience production keys and secrets are securely stored and protected using AWS KMS and Azure KeyVault. Secrets are encrypted at rest using schemes and key length compliant with FIPS140.2 and Nexthink internal cryptography policy.

A password policy has been designed and enforced on Nexthink's system based on standards like NIST Special Publication 800-63B and Nexthink risk context. Requirements contain, but are not limited to, length, maximum number of attempts, lockout, age, history, forbidden keywords, previously compromised passwords.

Nexthink leverage a password management solution to facilitate password and secrets management and reduce their exposure to potential threats.

3.14.1.6 Hardening

Nexthink provisions systems using IaC and pre-approved configurations as well as golden images approved by the security team to reduce the attack surface.

V6aaS gateways and Ubuntu-based platform VMs are hardened based on the Center for Internet Security (CIS) Benchmark and enforced with Ansible.

IT Infrastructure systems are hardened accordingly to identified risks.

3.14.1.7 Architecture

Production, pre-production, testing, and development environments are segmented either by dedicated Azure tenants or dedicated AWS accounts. Deliverables must follow the change management process to change from one environment to another.

In addition, AWS workloads are also segmented in different accounts based on functional requirements.

Security principles and requirements are embedded by design in the architecture as the Security team takes part of all architecture meetings. During the development process, the Definition of Done ensures designs are reviewed and validated. The Definition of Ready ensures no blind spot is left.

Nexthink implements zero-trust architecture principles

3.14.1.8 Asset management

Nexthink inventories its cloud and IT infrastructure assets within the information processing facility and ensures they have a clear owner so that they are accounted properly. Inventories are periodically reviewed to ensure completeness and accuracy.

User endpoints are centrally managed in a Mobile Device Management platform (MDM) to ensure change and configuration standardization.

Patch management is performed via update rings to ensure quality updates are deployed and endpoints availability. Security patches are rolled out accordingly to their severity as defined in the vulnerability management policy.

3.14.1.9 Endpoint security

Nexthink uses an Endpoint Detection and Response (EDR) platform on all corporate laptops. EDR capability encompass, but are not limited to, block advanced malware, exploits and fileless attacks, threats with behavioral threat protection, Artificial Intelligence, and cloud-based analysis. The EDR is reporting to the eXtended Detection and Response (XDR) platform to leverage correlation with firewall and authentication logs. Content update containing policies, new detection and protection engine and rules are deployed immediately upon availability.

Detected threats are reviewed and remediated daily. Upon analysis, a detected threat can become an incident and trigger the incident response process.

Nexthink implements restrictions to ensure that access to production environments is restricted to company managed devices.

Nexthink protects endpoint sensitive and critical data by enforcing encryption on removable storage devices. Provisioned laptops are full-disk encrypted using XTS-AES-128 or XTS-AES-256 when available with a 256-bits key length.

3.14.1.10 Email security

Nexthink uses Office 365 and relevant Microsoft security subscriptions including, but not limited to, Cloud Application Security, Phishing protection providing phishing detection, anti-spam, anti-spoof, and anti-impersonation. All Nexthink domains used to send emails are configured with SPF, DKIM and DMARC in quarantine mode.

Security awareness email campaigns are scheduled monthly, and results are analyzed through the KPI management. Emails campaigns scenarios includes phishing emails and fake malware as attachments.

3.14.1.11 Network controls

Nexthink implements network level protection for endpoints, systems, and applications via firewalls. Network is segmented in different building blocks in both Azure and AWS environments. Office networks, including wireless access, are segmented on a department level, and protected for internal business use only. More granular segmentation is implemented on a risk basis. Guest wireless access is provided on a separate logical network.

Nexthink uses IaC with pull request (PR) approvals to ensure that every change to network flows and controls are duly reviewed and approved.

Nexthink provides its employees and consultants with a VPN to access the corporate network remotely through an encrypted tunnel, using mutual authentication with server and client-side TLS certificates and enforced multi-factor authentication based on Duo MFA.

IP Whitelisting is implemented on critical systems to lower the exposure to potential threats. Inbound Internet traffic and internal network traffic of Nexthink Experience is protected by virtual private cloud networking and security groups.

Nexthink leverages Network Intrusion Detection Systems (NIDS) on IT infrastructure firewalls, all AWS accounts (excepted AWS organization master account) and Azure subscriptions including customer production environment.

Nexthink implements web application firewall technology to protects web resources from malicious attacks.

3.14.1.12 Physical Security

Nexthink has defined a set of security measures that are in place to protect information assets from security events associated with unauthorized physical access.

- Offices and server rooms are equipped with badging systems implementing:
  - Mifare DESFire EV1 cards.
  - Detection of forced-open doors and related physical attacks.
  - Time schedules based on roles.
- CCTV with motion detection to monitor and record access to office and server rooms entry points.
- Clean desk policy.
- Secure printing and disposal of hard copy materials.

Corporate IT Infrastructure does not process customer production data.

3.14.1.13 Data model

Nexthink Experience collects data using a lightweight agent based on patented technology. It captures and reports network connections, program executions, web requests, and many other activities and properties from employee devices on which it runs, the main data categories collected are the following:

Objects: Represents real life items recognized by Nexthink:

- User
- Device
- Package
- Application
- Executable
- Binary
- Port
- Destination
- Printer
- Domains

Activities: Represents actions performed by objects:

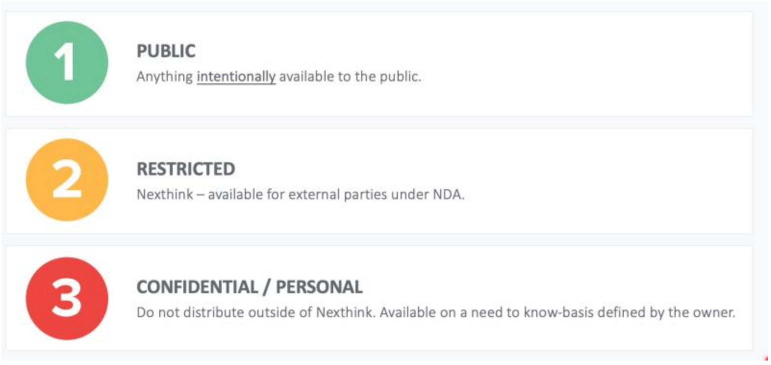
- Installation
- Execution
- Connection
- Print job
- System boot
- User logon
- Web request

Events are warnings or errors:

- Device warning
- Device error
- Execution warning
- Execution error

3.14.1.14 Data classification

Nexthink has defined Confidentiality policy that defines the classification levels of data based on their sensitivity, protection, and access requirements.



1 **PUBLIC**
Anything intentionally available to the public.

2 **RESTRICTED**
Nexthink – available for external parties under NDA.

3 **CONFIDENTIAL / PERSONAL**
Do not distribute outside of Nexthink. Available on a need to know-basis defined by the owner.

Confidential Information classification includes information that Nexthink is required to keep confidential, either by law, or under an agreement with a third party, such as a customer, reseller, or partner. This information should be protected against unauthorized disclosure or modification. Confidential information should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported.

3.14.1.15 Data protection

The Confidentiality policy defines de-classification scheme and classification levels, the information security policy defines the handling requirements

Customer data stored within the system is classified as confidential.

- **Inventory**: Data is inventoried and classified.
- **Restrict access to customer data**: Access to production environment to perform administrative actions is based on multi-factor authentication and bastion servers.
  - Creation and changes to privileged accounts in production environments follow formal change management using service request catalog.
  - Access is granted on demand, for a limited duration.
  - Access to systems components is controlled and restricted to those authorized personnel who have a legitimate need, such as the operations teams, support teams and the security team.
- **Segregation of environments**: Productive environment are completely segregated from nonproductive environments. This includes:
  - Dedicated tenants and accounts for the Cloud Environments.
  - Dedicated infrastructure and services for corporate systems.
- **Data in motion**: All communications to the cloud environment are encrypted using TLS 1.2 or above accordingly to the Cryptography Policy. This includes:
  - Communications between Collector to Cloud
  - Access to customer administrative interfaces
  - API access
  - Backups
  - Nexthink administrative access to cloud platform
- **Data at rest**: Data is encrypted at rest using native infrastructure as a service provider encryption capability using AES-256 server-side encryption.
- **Data retention:** The data retention policies define the retention applied to different, datasets, systems, and components. Transient and temporary data (or cache) is purged in a timely manner.

- **Data locations:** As part of the onboarding process, customer can select the main and associated secondary location used to store Nexthink Experience data.
- **Access to personal data**: Access to Personal data is restricted to only individuals with business need and protected by strong access control. Data attributes/items collected by the product are listed by category and marked as "Personal Data" and "Identifier", in the Data Inventory High Level documentation. During the Design Review, the security team provides requirements for how this data can be stored and transmitted, ensuring that proper compartmentalization and access control is in place. Personal data stays within the customer's production instance.
- **Data disposal**: Adequate measures are implemented to ensure data is securely disposed to avoid recoverable data.

3.14.2 Change management

Nexthink has implemented a change management process that is applicable to IT, Engineering, and Cloud Operations.

The following table shows types of changes and team mapping:

Change Type	IT	Engineering	Cloud Operations
Release of product and platform		✓	✓
Customer Change requests and Production Changes			✓
IT Infrastructure, software, and configuration	✓		
Emergency Changes	✓	✓	✓

3.14.2.1 Change Management process for Engineering

The change management process for Nexthink experience product is embedded in the Software Development lifecycle, following agile methodologies. The engineering and cloud operations teams, follow structured release process to design, develop, test, and approve releases. Code is developed, reviewed, and merged using standardized process to ensure required tests, approval and review are systematically performed.

Security requirements, tests, code reviews and validations are embedded in the process as defined in the Engineering Security Policy and supporting documentation. The Secure Coding Standard refers SANS Top 25 Most Dangerous Software Errors, OWASP Top 10 Web Application Security Risks, to provide the product context, and development teams' capabilities, and a list of mandatory high level security requirements.

Nexthink uses IaC with pull request approvals to ensure:

- Systems are standardized according to hardening requirements.
- Changes to system configuration, access control, network flows and controls are duly reviewed and approved.

- System patches are applied in a systematic way.

Once the feature is designed, acceptance criteria are defined (Definition of Ready) and, depending on specific criteria, a security design review is scheduled. Design reviews include, but are not limited to, security requirements review, threat modeling, penetration test planning, data classification, architecture documentation review.

Developers store the source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.

Source code, artifacts and third-party libraries dependencies are scanned for vulnerabilities and defects by Static Application Security Testing tools (SAST) and dependency scanners.

Product dependencies (open or closed source) are scanned with a Software Component Analysis (SCA) tool looking for potential security vulnerabilities and licensing issues.

Scan results are analyzed and planned for remediation as defined in the Definition of Done (DoD). The DoD is a common and shared definition of when a user story is fully done and encompasses all functional, User Experience, quality, security, and delivery requirements.

All releases are tested in non-productive environments (testing and pre-production) via Continuous Integration and Continuous Delivery (CI/CD) pipelines and validated by Quality Assurance team and Cloud platform team. The formal approval of the release is done by Engineering management Team. Deployment of the release is managed by the Cloud Operations Team following and agreed plan with Business and Customers.

3.14.2.2 Change Management process for Cloud Ops

Cloud Operations teams maintains, updates, and configures production environment following change management procedures. This includes customer requests performed through the official support platform - Zendesk.

3.14.2.2.1 Release of product and platform

Nexthink maintains a secure software development process, coding standards, and release strategy to ensure security is built-in to the products and applications.

Cloud infrastructure changes and software code deploys follow a defined change request process with automated and/or manual reviews and approvals.

Product updates are scheduled in waves to mitigate deployment risks:

- Preview wave: Demo and internal instances
- Wave 1: External demo, proof of value and customer UAT environments
- Wave 2: Small, mid-size customers
- Wave 3: Large customers

Notification of updates are sent to customers in advance before each wave to allow them to prepare for the update. The notification includes the release notes and updates. Nexthink Cloud releases follow the same quality process than on-prem versions. We additionally test all cloud related features and performance. The update method uses a blue/green deployment model, so the roll-back procedure is being tested on every product update as well as the backup infrastructure. There are automated checklists to validate that the upgraded environment is consistent and is working as expected.

3.14.2.2.2 Customer Change requests and Production Changes

Most of the configuration can be accomplished from the product interfaces (e.g., Portal, Finder). There are only specific configurations bounded to the platform (e.g., management of IP whitelists, enable/ disable assignment service) that must be performed by Support. There are standard procedures to process them with clear outcomes and low risk.

These changes can be requested to Support Team through established channels like the Product Support portal and by the dedicated email.

3.14.2.3 Change Management process for IT

IT systems follow a change management procedure that ensures that changes classified according to their impact, tested, reviewed, authorized, and duly documented.

The main docker image is rebuilt weekly to ensure containers based on this image are always up to date.

IT Infrastructure, software, and configuration

The IT team implements following change types: Standard, Major, Minor and Emergency changes.

Standard changes are pre-approved changes that have low impact and low risk. These changes occur periodically and follow a standard procedure. They do not follow the conventional process flow and it can be saved as a standard change template for reuse. Every time, approval is not required as these changes are evaluated and approved once initially.

Major changes are high impact and high-risk items that may alter production systems. This requires IT approval. This has a huge impact on ongoing business operations and has financial implications.

Minor changes are generally normal changes that do not have a major impact and are less risky to execute. These are non-trivial changes that do not happen frequently, but this undergoes every stage of change lifecycle including IT and security approval. It is important to document related information so that this can be converted to a standard change in future.

3.14.2.4 Emergency Changes

When an event has a direct impact on service levels (data ingestion, consumption, availability), emergency changes are implemented. Customers are notified at least 24 hours in advance in case of unplanned maintenance. Risk assessment is performed and roll back procedure is tested. Emergency changes can be triggered by Nexthink's monitoring or via other channels like customer support. Incident that triggered an emergency change are subject to postmortem including, but not limited to, root-cause analysis.

Recovery accounts are maintained to ensure emergency access to selected critical services.

If a bug has been discovered or a hot-fix is required in the platform (infrastructure) code, the Maintenance Release escalation process is followed based on the associated criticality and impact.

3.14.2.5 Change Management tools

Change management relies on the following tools to define, document, review, approve and record changes to systems, software components and configuration.

Atlassian ServiceDesk, Jira and Zendesk for customer relationship, they provide:

- Type of Change
- Risk impact evaluation
- Workflow capabilities, including approval and communication.
- Traceability and audit capabilities.

3.14.3 System operations

3.14.3.1 Incident management

Nexthink defines and maintain an operational monitoring to ensure the availability and performance of the solution. Incidents can be reported by multiple channels like email, phone, product support portal or by raised by the monitoring system.

Alert severities are defined to ensure prompt communication and acknowledgement by the Product Support and Cloud Ops teams. Upon validated alerts become incidents and are classified against four level: Low, Normal, High, and Urgent.

During the initial evaluation, once the impact and severity are identified (and correlated with other events) the engineer verify if the incident meets different scenarios criteria and trigger the relevant notification actions with different audience, frequency, channel, and owners. Example of scenarios are but not limited to degradation of a major feature, persistent performance problems, incident impacting multiple customers.

Upon resolution or mitigation of the incident, CloudOps will notify Support about the service restoration. Product Support will confirm with Customers (depending on scenario) that the service is restored, and the scenario is no longer applicable. Product Support will send a final communication closing the incident/escalation.

A root cause analysis is performed to ensure the incident has been fully understood, completely remediated, and will not reproduce along with a lesson-learned session to improve the process.

3.14.3.2 Security incident management

Nexthink has implemented an incident management policy and plan including:

- Roles and responsibilities
- Classification
- Communication Channels
- Tooling
- Reporting

- Playbooks for common incident types
- Test plans
- Lessons learned postmortem

Policy and plan are maintained and communicated to all Nexthinkers. The goal of the incident response process is to:

- Detect and address Information Security Incidents and the specific category data security breach.
- Reduce the impact of Information Security Incidents by ensuring an appropriate follow up.
- Help identify areas for improvement to decrease the risk and impact of future incidents.
- Provide a structure to all activities related to management of a Security Incident.
- Continuously improve our detection and response capability.

The plan defines a workflow to guide the general process through steps like preparation, detection, analysis, reporting, chain of custody, containment, eradication, recovery, and lessons learned.

Security incident can be raised internally or externally by customers respectively in dedicated channels embedded in the IT Support portal and the product support.

An incident responder is defined and depending on the importance of the incident, he/she assembles a team and coordinates all activities with stakeholders like service owners, Legal, IT team, forensic companies, etc.

Situational awareness is performed through regular touch point with all relevant staff.

Nexthink documents and maintains a process to investigate suspected data breaches and duly notify affected parties in accordance with applicable law and regulations. This includes a data breach notification procedure, communication template and a data breach specific procedure in the Security Incident Response Plan.

Communication is maintained during the incident to ensure providing our customers with the right level of information.

3.14.4 Additional description of controls relating to availability

Nexthink maintains a set of monitoring, assessment, and capacity management procedures to ensure the capacity of the Nexthink experience. This includes:

- Capacity and Performance Monitoring procedure for monitoring the usage of system resources.
- Monthly monitoring to measure SLA and SLO levels.
- Process to increase current capacity based on current usage, forecasts, and onboarding of new customers.
- Having have a rotating schedule of Cloud Operations Engineers to provide support for the weekends. 24x7 coverage from Monday-Friday including local bank holidays via the team distribution (India-Spain-US).

- Dedicated channels for the different alert severity to ensure efficient communication.

3.14.4.1 Disaster Recovery and Business Continuity plans
Business Continuity and Disaster Recovery Plans have been implemented including required processes and guidelines to performing an impact analysis and planning recovery activities in the event of incidents causing business disruption this includes:

- Annual Review of Business impact assessment and scenarios.
- Formal backup and restore procedures.
- Test strategy to validate, adapt and improve current plans.

3.14.4.2 Datacenters availability

- Azure Datacenter relies on availability sets and availability zones
- AWS containerized infrastructure is deployed in multiple regions and with at least 3 Availability zones.

3.14.4.3 Primary and secondary locations
Primary locations are used for service processing and platform management, relying on AWS and Azure datacenters built-in availability capabilities.

Secondary locations are used for backup purposes and rely on AWS and Azure datacenters built-in availability capabilities.

3.14.4.4 Backup and restore
Backups are performed at regular intervals and retained as defined in the Data Retention Policy. Backups are tested regularly and at least at every release.

3.15 Control activities

Nexthink maintains a set of policies and standard operating procedures to address security requirements and operate the cloud infrastructure. Nexthink’s SM, supported by the appropriate teams, implements controls related to security and availability Trust Services Criteria and develops relevant policies including internal standards (defining the good practices and guidelines to be followed by Nexthink teams) and operating procedures to allow the execution of the controls.

Policies are approved by the owners, annually reviewed by relevant staff, and centralized in a SharePoint available to all Nexthinkers. Changes in policies are communicated via Yammer. Procedures are documented in the relevant repositories like SharePoint or Confluence.

Relevant Policies, like the Global Anti-Bribery Policy, the IT Policy, the Acceptable Usage Policy, the Information Security Policy, the Travel and Expenses Policy and the Respectful Workplace Program – Anti-Harassment Policy and the Code of Conduct are sent to new employees to ensure acceptance and maintaining a secure and safe workplace. Before May 2022, the consultants were required to acknowledge the Acceptable Usage Policy. Post May 2022, the consultant management process was updated to ensure that the consultants also acknowledge the same set of policies as done by the new employees.

The tables below provide details about the policies and procedures applicable to the IT Corporate and Cloud Infrastructure Security:

Document	Purpose
Information Security Policy	Defines the security strategy and security requirements applicable to all Nexthink employees and systems. The aim of this document is to explain all the different measures that Nexthink has in place to ensure its own business continuity and recovery in case of a disaster.
Cloud Security Policy	The Information Security Policy describes high level security and privacy principles in the area of security engineering and software development. The present Cloud Security Policy aims to further explicit these domains for Nexthink Cloud offering.
Engineering Security Policy	Describes the high-level security principles applicable to Engineering and Software development and Operations.
Acceptable Usage Policy	Defines what constitutes an acceptable use of Nexthink's IT resources.
Confidentiality Policy	Describes the classification schemes and levels.
Data Retention Policy	Describes the retention applied to the different information managed by Nexthink.
Vulnerability Management Policy	Defines how Nexthink identifies and remediates vulnerabilities in its IT infrastructure, product, and Cloud offering.
Security Governance Policy	Defines security governance roles and responsibilities at Nexthink.
Security Incident Response Policy	Defines the handling of security incidents at Nexthink.
Business Continuity and Disaster Recovery Plan	Describes all the different measures that Nexthink has in place to ensure its own business continuity and recovery in case of a disaster.
Password Policy	Defines a set of rules designed to enhance computer security and employ strong passwords following security best practices.

Access Control Policy	Defines logical access control requirements at Nexthink including privileged account management.
Physical Security Policy	Describes the physical security controls applied in our offices but also in the data centers.
CCTV Policy	Defines the ground rules on how to manage and operate a "Closed-circuit television" system.
Cryptography Policy	Describes the standards and operational procedures used to produce, update and discard keys.
AWS Cloud Security Standard	Defines the AWS security standard across all Nexthink AWS accounts used for the Nexthink Experience product and supporting services.
AWS Services Secure Configuration Standard	Defines the security baseline for various AWS services. It is applicable for all production AWS accounts.
Secure Coding standard	Describes a set of security requirements to be implemented during development phase.
Documentation Procedure	Describes how documentation is managed.
Incident Notification Procedure	Describes how security incidents should be reported by Nexthink employees.
Incident Response Procedure	Describes how the Security Team identifies and responds to security incidents.
Third-party Management Policy	Describes how the Security Team manages third-party providers.
Third-party Assessment Procedure	Describes how the Security Team assesses the security posture of third-party providers.
Risk Management Procedure	Describes the risk management process.
Employee onboarding checklists	Describes the onboarding steps at Nexthink from an HR and IT perspective.
Employee offboarding checklists	Describes the offboarding steps at Nexthink from an HR and IT perspective.
Change management procedures	Describes the different change management process in place at Nexthink.

Backup and Recovery procedures	Describes the necessary steps for backing up and recovering the Nexthink Experience service as well as the IT Infrastructure components.
Disciplinary procedure	Describes the disciplinary process for policy infringements.

3.16 Communication and information

3.16.1 Internal communication

Nexthink has established different channels of communication so that everyone is informed of the company's current news and relevant updates.

Internal communication channels are presented during onboarding and documented in intranet. This to ensure a clear understanding of how internal communications functions at Nexthink, and best practices to keep in mind when communicating important messages with colleagues.

Nexthink Live is a monthly all-hands webinar where key information is shared from leadership and various departments to Nexthinkers in a direct, personal way. These meetings typically feature updates from our CEO and Co-founder Pedro Bados on Company progress and strategy; the product team on new product developments or demos; the CPO or the HR team on company policies or social initiatives; other departments in the company with important updates relevant to the broader team.

The NextUp@Nexthink Newsletter is a monthly bulletin sent to all employees. The newsletter includes a variety of content including social activities, employee spotlights, and other valuable, company-wide resources.

Yammer is an internal hub of information where team members can post updates, questions, resources and more. Yammer features different "communities" with unique objectives. Policy updates are communicated via Yammer.

Product and Engineering all-hands meeting is a weekly webinar where updates from the Product and the Engineering department are shared. Engineering all-hands meeting is organized every quarter to discuss yearly priorities and provide organizational updates.

Values and policies are communicated during welcome sessions and via the "Getting Started at Nexthink" learning path in the Nexthink Academy and are part of the mandatory employee starter package. Each employee must sign to acknowledge the policies prior to onboarding, including the Security governance policy which outlines their roles and responsibilities.

Confluence and SharePoint are the main documentation repositories used by IT, Engineering and Security.

Jira is used by the Security and Engineering team to organize security risk management and development tasks respectively.

Service Now (IT Service Management – ITSM module) is used by the Employees to report security incidents and IT Team to organize their daily work. The Security team uses ServiceDesk to organize its daily work.

3.16.2 External communication

Nexthink relies on a set of services to provide the necessary platform and product information to customers and partners.

- **Nexthink Support**: Support by phone and ticketing system available 24/7
- **Nexthink Academy training portal**: Help customers gain product knowledge.
- **Nexthink Community**: Enable customers to connect with users to exchange ideas, learn and network.
- **Nexthink Documentation**: Access product resources, including user manual, installation, and configuration guides.
- **Nexthink Library**: Leverage 100+ ready to use content packs and integrations to enhance Nexthink.

Nexthink runs a responsible disclosure program where customers and external security researchers are encouraged to responsibly disclose any vulnerability to Nexthink about its infrastructure or products and provided with clear guidelines and communication channels.

Nexthink maintains a process for customers to request/receive audits and compliance reports and evidence upon onboarding.

3.17 Risk assessment

Nexthink maintains a formal risk management program to continuously identify, assess, mitigate, and monitor relevant risks that could jeopardize the achievement of its principal service commitments and system requirements.

The scope of information security risk management is aligned with the scope of the ISMS and PIMS and Nexthink's overall risk management practice.

Nexthink is to perform relevant risk assessments on a yearly basis or when significant changes are proposed or occur.

The organization retains documented information of the results of the risk assessments.

Nexthink defines impact and likelihood criteria classification and based on this classification, top management has determined a risk score acceptance criteria aligned with business objectives as defined in the Governance and oversight section.

Nexthink's risk management program includes the following phases:

- **Identify:** Risk identification is triggered by annual risk assessment and monitoring, business impact analysis, ad-hoc observation, change management reviews, or third-party risk assessment or implementation. This step consists of identifying critical assets, and threats, and vulnerabilities associated with them.

- **Assess:** Identified risks are evaluated against their likelihood and impact, based on past security incidents, threat modeling report, reports from security or insurance companies, threat intelligence (experience and statistics, threat agent motivation, capabilities, and resources, perception of attractiveness and vulnerability of the asset, recent media attention), geographical factors (e.g., earthquake risk), existing controls and how effectively they reduce vulnerabilities. Likelihood and impact are evaluated against a scale to determine the risk score. A risk owner is defined and depending on the score, the risk is either modified, retained, avoided, or shared.

High level risks related to the service provided are approved by SM and reported during the Management Review.

3.18 Third-party management

Nexthink has implemented third-party risk management controls to identify, mitigate and monitor risks related to services provided by third parties. Risks are identified prior to onboarding a new vendor and reviewed biennially or upon major changes.

The Privacy and Cybersecurity committee and the Security team evaluates new services against Nexthink's privacy and security requirements including Confidentiality, Availability, and Integrity. The Security team analyzes and documents third-party risk posture, including the review of SOC2 controls reports, ISO 270XX or equivalent certifications, or self-assessment questionnaires like CAIQ or Vendor Security Assessment Questionnaire (VSAQ). Identified risks are tracked and treated accordingly to the risk management process. Risks are reviewed on a yearly basis as a part of monitoring risks. Risk availability requirements are monitored and monthly through KPIs, and analyzed for implementing corrective action to remediate defects, if required.

The privacy team has established a Data Privacy Agreement and ensures any other privacy, legal or security provision are present in the service contract.

Once validated by both teams, the third-party service can be used by Nexthink.

3.19 Monitoring activities

3.19.1 Risk monitoring

In collaboration with asset's owner and/or head of business units, risks are re-evaluated to ensure suitability, adequacy, and effectiveness of existing controls.

Third-party risks are re-evaluated on a yearly basis based on review of the updated documentation (SOC 2, ISO, Security policies) and review of the risk associated with each provider to ensure that risk has been assessed according to the data processed or the security measures in place.

3.19.2 Key Performance Indicators

Key Performance Indicators (KPI) are defined to measure the compliance and/or effectiveness of controls. They are periodically collected, analyzed, and reviewed. KPI analysis is helping the decision-making process to determine the compliance and/or effectiveness of a security control and drive a remediation action or the security roadmap.

3.19.3 Threat Intelligence monitoring, vulnerability scanning and monitoring

The SEC team is subscribed to newsfeeds to stay up to date with the latest threat intelligence news related to threats and security risks that might impact Nexthink.

Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure, and the IT Infrastructure. Findings are centrally managed in the Vulnerability Management platform. Vulnerability scanning is performed automatically, and findings are evaluated for remediation on a weekly basis.

3.19.4 Security testing

Penetration testing is conducted to measure the security posture of IT's infrastructure. Different scenarios are tested, from the stolen laptop or external attacker to a disgruntled employee or an attacker that has obtained access to the internal network.

Application Penetration Testing are performed to identify vulnerabilities and provide deeper insight, through demonstration, into the business risks of various vulnerabilities. Application penetration tests are performed accordingly to the Engineering Security Policy. Nexthink leverages different type of approach like Blackbox, Greybox or, Whitebox testing.

An independent security company is mandated to perform the audits. The selected company uses an accepted industry standard penetration testing methodology specified by Nexthink. Identified vulnerabilities are evaluated against their severity and likelihood to determine a score. The score is used to ensure vulnerabilities are remediated in a timely manner. Once vulnerabilities are remediated, the validation is scheduled in the next penetration test.

3.19.5 Cloud Security Posture Management

Nexthink continuously scans resources deployed in AWS accounts to ensure they are aligned with the Nexthink AWS Services Secure Configuration Standard and deviations are reported and acted upon.

3.19.6 Compliance monitoring

3.19.6.1 Internal audit

Internal Audit (IA) is responsible for assessing the Nexthink’s control environment through rigorous evaluation of operational and administrative controls, policies, and procedures.

A sampling of the security measures mapped to ISO 27001:2013 / 27017:2015 / 2018:2019 / 27701:2019 annexes are assessed during the annual IA to ensure that internal controls are designed and operating adequately.

IA is mandated by the SEC team and is reporting to the SM. IA communicates significant findings and the status of corrective actions directly to the SM. IA adheres to standards of moral and ethical conduct, including those set forth in the code of conduct.

3.19.6.2 External audit

Nexthink undergoes yearly surveillance audit focused on ISMS and PIMS scope. Nonconformities are reported to the SM and duly remediated following the improvement process.

3.19.7 Security monitoring

The Information Security Policy and the Cloud Security policy describe the information required to be captured in logs.

Security-relevant logs are collected centrally to ensure they can be efficiently queried and cannot be tampered with, including endpoint protection logs, AWS CloudTrail, Azure audit logs, and application-level security events.

Logs stored into the SIEM solution are validated against integrity checks and retained based on the retention policy. Alerts are defined based on detection use-cases and are reviewed on a daily or weekly basis.

A commercial Managed Detection and Response (MDR) provider ensure continuous monitoring based on defined detection scenarios.

3.19.8 Improvement process

Identified control deficiencies are communicated to parties responsible for taking corrective action. Root cause analysis is performed, and remediation plans are proposed and monitored through resolution.

3.19.9 Risk mitigation

Mitigate: Unless the risk is retained, a risk treatment plan must be defined to lower the residual risk to the acceptance level. Once selected and an owner defined, the different measures are implemented in coordination with the relevant Nexthink teams. Measures are mapped against the different standards such as SOC2 Trusted Service Criteria or ISO 270XX Annex A.

Continuous improvement: As part of our continuous improvement process, the risk process, methodology, evaluation, and criteria are reviewed on a yearly basis.

Cyber insurance: As part of the global insurance policy renewal, coverage and policies related to cyber risks are reviewed and adapted based on the current context.

3.20 Controls implemented to support the applicable trust services criteria

The controls supporting the applicable Trust Services Criteria are included in section 4 (“Common Criteria, related controls and tests of controls”) of this report. Although the applicable trust services criteria and related controls are included in section 4, they are an integral part of Nexthink’s description of its Solution.

3.21 Complementary subservice organizations control

Nexthink relies on third parties to deliver Nexthink Experience and are not included within the scope of this examination.

The table below shows the Complementary Subservice Organization Controls (CSOC) under the responsibility of any third parties mandated by Nexthink:

Applicable Trust Services Criteria	Complementary Subservice Organization Controls
CC1; CC2; CC3; CC4; CC5; CC9	Subservice organizations are responsible for the definition, implementation, communication, monitoring and maintenance of an appropriate internal control environment, risk management, governance, application of a code of conduct, personnel and vendors selection process and training related to their own personnel and/or their own service providers when impacting the in-scope Service Organization’s systems.
CC6	Subservice organizations are responsible for defining appropriate access control policies and procedures regarding their own users, including users provisioning, deprovisioning, recertification and monitoring of sensitive users’ activities, and defining, implementing, maintaining, and monitoring appropriate security configurations and protection of their systems when impacting the in-scope Service Organization's systems.
CC7	Subservice organizations are responsible for implementing adequate security events detection and security incident management and remediation procedures, including cyber resilience and continuity, related to their own personnel and to their own systems when impacting the in-scope Service Organization's systems.
CC8	Subservice organizations are responsible for adequately defining, implementing, and maintaining a process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software, and procedures) related to their own systems when impacting the in-scope Service Organization's systems.
A1	Subservice organizations are responsible for the appropriate maintenance, monitoring, evaluation, and adaptation of processing capacity, including recovery related to their own systems used when impacting the in-scope Service Organization's systems.

The table below shows the Complementary Subservice Organization Controls under the responsibility and specific to AWS:

Applicable Trust Services Criteria	**AWS Complementary Subservice Organization Controls**
CC2.2; CC2.3; CC6.7	**AWSCA-1.6**: KMS- Specific – Roles and responsibilities for KMS cryptographic custodians are formally documented and agreed to by those individuals when they assume the role or when responsibilities change.
CC2.1; CC3.1; CC3.2; CC3.3; CC3.4; CC4.1; CC4.2; CC5.1; CC5.2; CC5.3; CC9.1; CC9.2; A1.2	**AWSCA-1.10**: AWS has a process in place to review environmental and geo-political risks before launching a new region.
CC6.2; CC6.3	**AWSCA-2.1**: User access to the internal Amazon network is not provisioned unless an active record is created in the HR System by Human Resources. Access is automatically provisioned with least privilege per job function. First time passwords are set to a unique value and changed immediately after first use.
CC6.2; CC6.3; CC6.7; CC6.8	**AWSCA-2.2**: IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.
CC6.1; CC6.2; CC6.3; CC6.7; CC6.8	**AWSCA-2.3**: IT access privileges are reviewed on a periodic basis by appropriate personnel.
CC6.1; CC6.2; CC6.3	**AWSCA-2.4**: User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.
CC6.1	**AWSCA-2.5**: Password configuration settings are managed in compliance with Amazon.com's Password Policy.
CC6.1; CC6.6	**AWSCA-2.6**: AWS requires two-factor authentication over an approved cryptographic channel for authentication to the internal AWS network from remote locations.
CC6.1; CC6.6; CC7.1; CC8.1	**AWSCA-3.1**: Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.

CC2.1; CC7.1; CC8.1	**AWSCA-3.6**: AWS performs application security reviews for externally launched products, services, and significant feature additions prior to launch to evaluate whether security risks are identified and mitigated.
CC6.1; CC6.6;	**AWSCA-3.7**: S3- Specific – Network devices are configured by AWS to only allow access to specific ports on other server systems within Amazon S3.
CC6.1; CC6.6;	**AWSCA-3.8:** S3-Specific – _External data access is logged with the following information: data accessor IP address, object and operation. Logs are retained for at least 90 days.
CC6.1; CC6.6	**AWSCA-3.9**: EC2- Specific – Physical hosts have host-based firewalls to prevent unauthorized access.
CC6.1	**AWSCA-3.10**: EC2- Specific – Virtual hosts are behind software firewalls which are configured to prevent TCP/IP spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.
CC6.1	**AWSCA-3.11**: EC2- Specific – AWS prevents customers from accessing custom AMIs not assigned to them by a property of the AMI called launch- permissions. By default, the launch- permissions of an AMI restrict its use to the customer/account that created and registered it.
CC6.1	**AWSCA-3.12**: EC2- Specific – AWS prevents customers from accessing physical hosts or instances not assigned to them by filtering through the virtualization software.
CC6.1	**AWSCA-3.13**: VPC- Specific – Network communications within a VPC are isolated from network communications within other VPCs.
CC6.1	**AWSCA-3.14**: VPC- Specific – Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways.
CC6.1	**AWSCA-3.15**: VPC- Specific – Internet traffic through an Internet Gateway is forwarded to an instance in a VPC only when an Internet Gateway is attached to the

	VPC, and a public IP is mapped to the instance in the VPC.
CC6.7	**AWSCA-4.1**: EC2- Specific – Upon initial communication with an AWS-provided Linux AMI, AWS enables secure communication by SSH configuration on the instance, by generating a unique host-key and delivering the key's fingerprint to the user over a trusted channel.
CC6.7	**AWSCA-4.3**: VPC- Specific – Amazon enables secure VPN communication to a VPN Gateway by providing a shared secret key that is used to establish IPSec Associations.
CC6.1; CC6.7	**AWSCA-4.4**: S3- Specific – S3 generates and stores a one-way salted HMAC of the customer encryption key. This salted HMAC value is not logged.
CC6.1	**AWSCA-4.5**: KMS- Specific – Customer master keys used for cryptographic operations in KMS are logically secured so that no single AWS employee can gain access to the key material.
CC6.1; CC6.7	**AWSCA-4.6**: KMS- Specific – AWS Services that integrate with AWS KMS for key management use a 256-bit data key locally to protect customer content.
CC6.1; CC6.7	**AWSCA-4.7**: KMS- Specific – The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES master key unique to the customer's AWS account.
CC6.1	**AWSCA-4.8**: KMS- Specific – Requests in KMS are logged in AWS CloudTrail.
CC6.1; CC6.7	**AWSCA-4.9**: KMS- Specific – KMS endpoints can only be accessed by customers using TLS with cipher suites that support forward secrecy.
CC6.1	**AWSCA-4.10**: KMS- Specific – Keys used in AWS KMS are only used for a single purpose as defined by the key usage parameter for each key.
CC6.1; CC6.7	**AWSCA-4.11**: KMS- Specific – KMS keys created by KMS are rotated on a defined frequency if enabled by the customer.

CC6.1; CC6.4	**AWSCA-4.12**: KMS- Specific – Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
CC6.1; CC6.4	**AWSCA-4.13**: KMS- Specific – Access attempts to recovery key materials are reviewed by authorized operators on a cadence defined in team documentation.
CC6.1; CC6.6; CC6.7	**AWSCA-4.14**: KMS-Specific – The production firmware version of the AWS Key Management Service HSM (Hardware Security Module) has been validated with NIST under the FIPS 140-2 standard or is in the process of being validated.
CC6.4; CC6.7	**AWSCA-5.1**: Physical access to data centers is approved by an authorized individual.
CC6.4; CC6.7	**AWSCA-5.2**: Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
CC6.4; CC6.7	**AWSCA-5.3**: Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
CC6.4	**AWSCA-5.4**: Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
CC6.4; A1.2	**AWSCA-5.5**: Access to server locations is managed by electronic access control devices.
CC7.2; CC7.3; A1.2	**AWSCA-5.6**: Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
A1.2	**AWSCA-5.7**: Amazon-owned data centers are protected by fire detection and suppression systems.
A1.2	**AWSCA-5.8**: Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.

A1.2	**AWSCA-5.9**: Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owned data centers and third-party colocation sites where Amazon maintains the UPS units.
A1.2	**AWSCA-5.10**: Amazon-owned data centers have generators to provide backup power in case of electrical failure.
CC7.3; CC7.4; CC7.5; CC9.2; A1.2	**AWSCA-5.11**: Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units (unless maintained by Amazon), and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
CC3.2; CC3.3; CC3.4; CC4.1; CC7.3; CC7.4; CC7.5; CC9.2; A1.2	**AWSCA-5.12**: AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
CC6.5; CC6.7; C1.2	**AWSCA-5.13**: All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
CC6.1; CC6.8; CC7.5; CC8.1	**AWSCA-6.1**: AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service.
CC6.8; CC8.1	**AWSCA-6.2**: Change details are documented within one of Amazon's change management or deployment tools.
CC6.8; CC8.1	**AWSCA-6.3**: Changes are tested according to service team change management standards prior to migration to production.
CC6.8; CC8.1	**AWSCA-6.4**: AWS maintains separate production and development environments.
CC6.8; CC8.1	**AWSCA-6.5**: Changes are reviewed for business impact and approved by authorized personnel prior to

	migration to production according to service team change management standards.
CC6.8; CC7.1; CC8.1	**AWSCA-6.6**: AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution.
CC8.1	**AWSCA-6.7**: Customer information, including personal information, and customer content are not used in test and development environments.
CC6.7	**AWSCA-7.1:** S3-Specific – S3 compares user provided checksums to validate the integrity of data in transit. If the customer provided MD5 checksum does not match the MD5 checksum calculated by S3 on the data received, the REST PUT will fail, preventing data that was corrupted on the wire from being written into S3.
A1.2	**AWSCA-7.3:** S3-Specific – When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
A1.2	**AWSCA-7.4:** S3-Specific – Objects are stored redundantly across multiple fault-isolated facilities.
A1.2	**AWSCA-7.5:** S3-Specific – The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
A1.2	**AWSCA-7.6:** RDS-Specific – If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
CC6.5	**AWSCA-7.7:** AWS provides customers the ability to delete their content. Once successfully removed the data is rendered unreadable.
CC6.5	**AWSCA-7.8:** AWS retains customer content per customer agreements.
CC7.1	**AWSCA-7.10:** EC2- Specific - Amazon EC2 enables clock synchronization based on Network Time Protocol in EC2 Linux instances, to achieve accuracy within 1 millisecond of Coordinated Universal Time

CC2.1; CC6.1; CC6.6; CC6.8; CC7.2; CC7.3; CC7.4; A1.1; A1.2	**AWSCA-8.1**: Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
CC2.1; CC6.1; CC6.6; CC6.8; CC7.2; CC7.3; CC7.4; CC7.5; CC8.1; A1.2	**AWSCA-8.2**: Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
CC2.2; CC2.3	**AWSCA-9.1**: AWS maintains internal informational websites describing the AWS environment, its boundaries, user responsibilities and services.
CC1.1; CC1.4	**AWSCA-9.2**: AWS conducts pre-employment screening of candidates commensurate with the employee’s position and level, in accordance with local law and the AWS Personnel Security Policy.
CC6.1; CC6.8; CC7.1; CC8.1	**AWSCA-9.4**: AWS host configuration settings are monitored to validate compliance with AWS security standards and automatically pushed to the host fleet.
CC2.3	**AWSCA-9.5**: AWS provides publicly available mechanisms for customers to contact AWS to report security events and publishes information including a system description and security and compliance information addressing AWS commitments and responsibilities.
CC1.2; CC2.1; CC3.1; CC4.1; CC4.2;	**AWSCA-9.8**: AWS has established a formal audit program that includes continual, independent internal and external assessments to validate the implementation and operating effectiveness of the AWS control environment.
CC1.4;	**AWSCA-9.9**: AWS has a process to assess whether AWS employees who have access to resources that store or process customer data via permission groups are subject to a post- hire background check as applicable with local law. AWS employees who have access to resources that store or process customer data will have a background check in accordance to the AWS Personnel Security Policy.

A1.2	**AWSCA-10.1**: Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
A1.2; A1.3	**AWSCA-10.2**: Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
CC2.2; CC3.2; CC3.3; CC3.4; CC5.3; CC7.3; CC7.4; CC7.5; CC9.1; A1.1; A1.2; A1.3	**AWSCA-10.3**: AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
A1.1; A1.2	**AWSCA-10.4**: AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.
CC1.1; CC1.4; CC2.2; CC2.3; CC9.2	**AWSCA-11.1**: Vendors and third parties with restricted access, that engage in business with Amazon are subject to confidentiality commitments as part of their agreements with Amazon. Confidentiality commitments included in agreements with vendors and third parties with restricted access are reviewed by AWS and the third party at time of contract creation or renewal.
CC1.1; CC1.4; CC2.3; CC4.1; CC9.2	**AWSCA-11.2**: AWS has a program in place for evaluating vendor performance and compliance with contractual obligations.
CC2.2; CC2.3; CC9.2	**AWSCA-11.3**: AWS communicates confidentiality requirements in agreements when they are renewed with vendors and third parties with restricted access. Changes to standard confidentiality commitments to customers are communicated on the AWS website via the AWS customer agreement.

3.21.1 Infrastructure as a Service Providers for Core Services:

- **Microsoft Corporation "Azure**" is the public cloud computing platform offering of Microsoft which offers software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

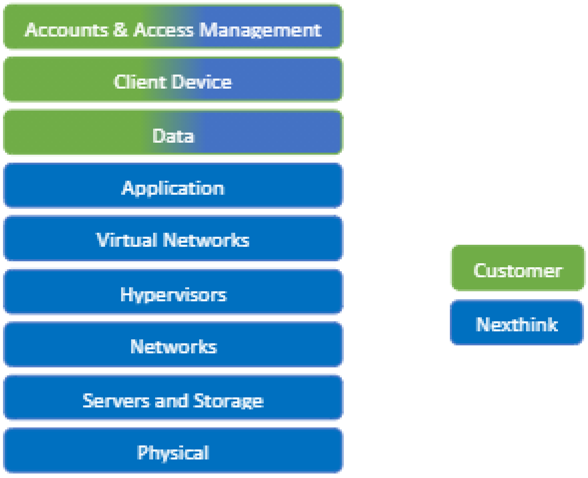
- **Amazon Web Services EMEA SARL (AWS)** is the public cloud computing platform offering of Amazon which offers software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS).

3.21.2 Non-Core Services

- **Zendesk:** Main support platform designed to ensure support capabilities and interaction platform with Nexthink Customers.
- **Okta:** Identity as a Service provider used to deliver corporate and product Single Sign-On capabilities.

3.22 Complementary User Entity Controls for Nexthink customers (shared responsibility model)

Nexthink has created a responsibility map based on the Software-as-a-Service model where the different areas of responsibility can be clearly identified:



Complementary User Entity Control	Relevant SOC2 Control Criteria
CUEC-01: User Entities are responsible for granting access to the service, granting the appropriate permissions to the users, API keys and any other security mechanisms based on the RBAC capabilities, as well as managing the lifecycle of these identities.	CC6.1, CC6.2, CC6.3, CC6.6, CC7.4
CUEC-02: User entities are responsible for ensuring that user entities' systems have access to service side components of Nexthink and that the required security controls defined in the security policy have been applied.	CC4.1, CC6.1, CC6.6, CC6.7

CUEC-03: Devices used to consume Nexthink Cloud through Portal, Finder or API integrations are managed by the user entity and, as such, necessary security controls must be implemented by the user entity.	CC6.1, CC6.7
CUEC-04: User entities are responsible for managing data classification according to its internal classification policies. User entities also needs to validate applicable requirements to the datasets used by Nexthink.	CC6.1, CC7.3
CUEC-05: Any data collected by a customized script is the responsibility of the User Entities.	CC6.1, CC7.3
CUEC-06: User Entities are responsible of the configuration of the monitored domains and transactions.	CC6.1, CC7.3
CUEC-07: User Entities are responsible for the timely, correct, and complete execution of the customer User-Acceptance Testing.	CC8.1
CUEC-08: User Entities are responsible for performing the necessary verifications or request from Nexthink teams any relevant additional information to verify the appropriateness of the configuration changes, before approving the change implementation.	CC8.1
CUEC-09: User Entities are responsible for anonymizing data provided to Nexthink and/or not inputting real data in the non-production environments (e.g., test, pre-production, support ticket, etc.).	CC8.1
CUEC-10: User Entities are responsible for adequately communicating to their Management and to Nexthink about the nature of security incidents, related to their personnel and own resources impacting used Nexthink solutions.	CC7.4

CUEC-11: User Entities are responsible for detecting unauthorized changes to endpoints' configuration and review the relevant security inputs provided by Nexthink (e.g., binaries, remote action parameters, etc.)	CC6.8
CUEC-12: User Entities are responsible for monitoring the API usage via the API Audit trail functionality.	CC7.2, CC7.3
CUEC-13: User Entities are responsible for implementing adequate security events detection and security incident management and remediation procedures, including cyber resilience and continuity, related to their own personnel and to their own systems used to connect to the in-scope Nexthink's systems.	CC7.4
CUEC-14: User Entities are responsible for the definition, implementation, communication, monitoring and maintenance of an appropriate internal control environment, risk management, governance, application of a code of conduct, personnel and vendors selection process and training related to their own personnel and/or their own service providers using the in-scope Nexthink's systems.	CC1.1-CC1.5, CC2.1-CC2.3, CC3.1-CC3.4, CC4.1-CC4.2, CC5.1-CC5.3, CC9
CUEC-15: User Entities are responsible for the appropriate maintenance, monitoring, evaluation, and adaptation of processing capacity, including recovery related to their own systems used to connect the in-scope Nexthink's systems.	A1.1-A1.2

4 Description of Trust Service Criteria, Controls, Tests and Results of Tests

The examination was conducted in accordance with the security and availability principles as set forth in TSP Section 100, 2017 Trust Services Criteria For Security, Availability, Processing Integrity, Confidentiality, and Privacy, (AICPA, Trust Services Criteria) (Technical Practice Aids) ("applicable trust services criteria"), DC Section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report ("description criteria"), of the American Institute of Certified Public Accountants (AICPA) and the International Standard on Assurance Engagements 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board.

Our testing of Nexthink's controls was restricted to the controls identified by Nexthink to meet the criteria for the security and availability principles listed in chapter 4 of this report and was not extended.

Although the applicable trust services criteria and related controls are presented in this chapter, they are, nevertheless, an integral part of Nexthink's description of its Nexthink Experience System throughout the period 15th December 2021 to 15th June 2022.

a) Performed and Results of Tests of Controls

In planning the nature, timing, and extent of our testing of the controls specified by Nexthink, we considered the aspects of Nexthink's control environment, risk assessment processes, communication and management monitoring procedures and performed such procedures as we considered necessary in the circumstances.

b) Testing Performed and Results of Tests

Tests performed of the operational effectiveness of the Controls detailed in this chapter are described below:

Type of Test	Description
Re-performance	Re-performed application of the control policy or procedure.
Inspection	Inspected documents and reports indicating performance of the control policy or procedure.
Inquiry	Made inquiries of appropriate personnel and corroborated responses with Management of Nexthink.
Observation	Observed application of specific controls.

4.1 Part A: Trust Service Criteria and Control Activities provided by Nexthink

Criteria Common to All Security, Availability, Processing Integrity, and Confidentially Principles

4.1.1 CC1.0 – Common Criteria related to Control Environment

Criteria	Nexthink Control
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**ID 020 - Code of Conduct and Acceptable Use of End-user Computing** Acceptable use policy and code of Conduct is in place to guide the organization's personnel on the proper use of information assets and their roles and responsibilities. Ensure both policies are disseminated to all employees. Contracts include confidentiality clause.
	ID 038 - Employee performance review process Ensure that a formal process to measure employee performance is implemented.
	ID 065 - Non-Compliance Investigation, Sanctions and Disciplinary process Ensure that a disciplinary process is implemented and applied according to the company policy.
	ID 089 - Security & Privacy Governance Program Nexthink's security and privacy program maintains documentation of high-level policies and lower level controls and procedures. The policies and procedures cover the design, development, implementation, operation, maintenance and monitoring of in-scope systems. Controls are developed and maintained following objectives, risk assessments, compliance or customer requirements.
	ID-091: Security Awareness & Trainings Nexthink provides its employee with mandatory initial and continuous security awareness training, aligned to the sensitivity of the data and systems they are required to perform their job duties.
	ID-110: Understanding the Policies and Controls/Procedures Different documents used as part of the information Security Management System are clearly defined and documented. Ensure that all documents used in the ISMS follow the documentation procedure.

Criteria	Nexthink Control
	ID-113: Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**ID-014: Board of directors** A Board Charter outlines the roles, responsibilities, and authorities of the Board of Directors (individually and collectively).
	ID-057: Management leadership Ensure business-oriented objectives and results are reported to the management. Committees are held as defined in the Security Governance policy.
	ID-059: Metrics Measurements and Continuous Monitoring Metrics are defined to measure the effectiveness of controls and they are continuously monitored. KPIs are reviewed annually by the Security team to ensure accuracy and completeness.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**ID-047: HR Management and Reporting** HR maintains an inventory of job descriptions defined and duly approved and accepted by employees.
	ID-090: Security & Privacy Roles and Responsibilities Security roles and responsibilities are defined and communicated for all personnel. Security governance policy and Acceptable usage policy defines roles and responsibilities.
	ID-093: Security Objectives, Architecture and Design Nexthink documents its security architecture, including system and infrastructure security diagrams. Security principles and high-level security best practices are embedded in Nexthink's security strategy, and used as a reference when designing, implementing, and operating our Information Security Management System. Ensure during creation and review of Cloud Security policy and Engineering policy that these principles are present and updated if required.

Criteria	Nexthink Control
	ID-102: Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.
	ID-113: Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**ID-009: Audit Related Training Education Awareness and Responsibilities** Employees are informed and trained on the organization's monitoring and auditing process. Training is reviewed on a yearly basis or upon changes.
	ID-012: Background Check Reviews Nexthink employees undergo systematic background screening prior to employment. The checks performed are aligned to the risk associated to the job position. Background checks are performed by the third-party HireRight.
	ID-014: Board of directors A Board Charter outlines the roles, responsibilities, and authorities of the Board of Directors (individually and collectively).
	ID-021: Competences Nexthink provides employees the opportunity to attend conferences, access to training courses, studies to maintain and further advance their skills relevant to their job functions and business objectives.
	ID-038: Employee performance review process Ensure that a formal process to measure employee performance is implemented.
	ID-088: Security & Privacy Documentation Management The Policy Management Process describes how the documentation relevant to the Information Security Management System (ISMS) is governed, managed, maintained, and disseminated. Documents are re-viewed on a yearly basis following the Documentation Procedure.

Criteria	Nexthink Control
	ID-091: Security Awareness & Trainings Nexthink provides its employee with mandatory initial and continuous security awareness training, aligned to the sensitivity of the data and systems they are required to perform their job duties.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**ID-002: Access Establishment Modification and Termination** Nexthink's HR Operations and IT teams deprovision user access upon employees leaving the company. Nexthink new-hires on-boarding is coordinated between HR and IT to ensure appropriate access provisioning and system configurations are in place for each new hire. The HRIS system (BambooHR) sends automated notifications to the IT ServiceDesk prior to employee onboarding.
	ID-014: Board of directors A Board Charter outlines the roles, responsibilities, and authorities of the Board of Directors (individually and collectively).
	ID-037: Employee Incentives and Rewards Employees receive regular peer recognition, feed-back and rewards for positive behavior and impact.
	ID-038: Employee performance review process Ensure that a formal process to measure employee performance is implemented.
	ID-047: HR Management and Reporting HR maintains an inventory of job descriptions defined and duly approved and accepted by employees.
	ID-065: Non-Compliance Investigation, Sanctions and Disciplinary process Ensure that a disciplinary process is implemented and applied according to the company policy.
	ID-090: Security & Privacy Roles and Responsibilities Security roles and responsibilities are defined and communicated for all personnel. Security governance policy and Acceptable usage policy defines roles and responsibilities.

4.1.2 CC2.0 - Common Criteria Related to Communication and Information

Criteria	Nexthink Control
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	**ID-005: Application Security Testing** Application penetration tests are performed according to the defined Engineering Security policy.
	ID-007: Asset management Nexthink inventories its assets within the information processing facility and ensures they have a clear owner so that they are accounted properly. IT maintains an asset inventory system for their in-scope assets. An annual review of the account owner is per-formed.
	ID-008: Audit program The organization performs manual testing and reviews of systems, accounts and controls as needed. The audit may be performed by internal teams or external auditors. The organization has defined auditing processes including system configuration monitoring, activity monitoring, access review, and controls compliance audit and results are reported to senior management. Metrics are defined to measure the effectiveness of controls and they are reported to/reviewed by senior management.
	ID-018: Centralized Security Information and Event Management The Information Security Policy and the Cloud Security policy describe the information required to be captured in logs. Security-relevant logs are generated both at the cloud provider level and at the application level, ensuring security-relevant events are logged and centralized to ensure they can be efficiently queried and cannot be tampered with, including antivirus logs, AWS CloudTrail, Azure audit logs, and application-level security events.

Criteria	Nexthink Control
	ID-028: Data Classification Ensure that the definition and classification level are in place for different datasets used. Ensure that the Confidentiality Policy contains the different relevant classification levels. Ensure that Engineering Security Policy supports the definition of data sets according to data classification. Ensure that the Cloud Security Policy contains data handling process including: - Encryption Requirements - Access Controls Ensure that the data retention policy sets retention requirements according to different datasets.
	ID-029: Data Deletion Procedures - Data Retention Ensure that retention is enabled in the different components and technologies used in the Cloud Environment.
	ID-031: Data Inventory and Lifecycle Management Data is classified according to its classification, and its lifecycle is defined. Transient and temporary data (or cache) is purged in a timely manner. The Data Classification and Data Inventory has been reviewed during the last year.
	ID-045: Free and Open-Source Software (FOSS) Security Product dependencies (open or closed source) are scanned with a Software Component Analysis (SCA) tool looking for potential security vulnerabilities and licensing issues.
	ID-059: Metrics Measurements and Continuous Monitoring Metrics are defined to measure the effectiveness of controls and they are continuously monitored. KPIs are reviewed annually by the Security team to ensure accuracy and completeness.
	ID-076: Privacy Terms and Consent Notices Ensure that the following requirements are duly documented and agreed by customers in the Contractual Agreements: - Privacy terms- Consents- Intended use- Notices- 3rd party Sub-processors

Criteria	Nexthink Control
	ID-081: Responsible Disclosure Process Nexthink runs a responsible disclosure program where customers and external security researchers are encouraged to responsibly disclose any vulnerability to Nexthink about its infrastructure or products and provided with clear guidelines and communication channels.
	ID-093: Security Objectives, Architecture and Design Nexthink documents its security architecture, including system and infrastructure security diagrams. Security principles and high-level security best practices are embedded in Nexthink's security strategy, and used as a reference when designing, implementing, and operating our Information Security Management System. Ensure during creation and review of Cloud Security policy and Engineering policy that these principles are present and updated if required.
	ID-102: Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.
	ID-106: Threat Intelligence Monitoring Stay up to date with the latest threat intel news related to threats and security risks that might impact Nexthink. The Security Team subscribes to news, feeds, forums, and special interest groups to receive updates on threat-intelligence and updates on applicable regulations and compliance.
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.	**ID-008: Audit program** The organization performs manual testing and reviews of systems, accounts and controls as needed. The audit may be performed by internal teams or external auditors. The organization has defined auditing processes including system configuration monitoring, activity monitoring, access review, and controls compliance audit and results are reported to senior management. Metrics are defined to measure the effectiveness of controls and they are reported to/reviewed by senior management.

Criteria	Nexthink Control
	ID-009: Audit Related Training Education Awareness and Responsibilities Employees are informed and trained on the organization's monitoring and auditing process. Training is reviewed on a yearly basis or upon changes.
	ID-019: Change Management Nexthink has defined a change management process defining the different type, approval workflow and review. System management tools are provisioned following the same requirements and configurations as any production system. - All changes must go through pull requests with code reviews. - Deployment happens in the same way as for the product components themselves, through build pipelines. - Cloud system management tools are developed according to the SDLC (including Definition of Ready and Definition of Done)
	ID-026: Data Breach Notification Nexthink documents and maintains a process to investigate suspected data breaches and duly notify affected parties in accordance with applicable law and regulations. This includes a data breach notification procedure and communication template and a data-breach specific procedure in the security incident response plan. The following procedures are available, approved and up to date: - Information Security Incident Response Plan - Personal Data Breach Notification
	ID-051: Improvement process Identified control deficiencies are communicated to parties responsible for taking corrective action. Root cause analysis is performed, and remediation plans are proposed and monitored through resolution.
	ID-053: Internal Business Communications Ensure that formal communication channels are defined and communicated to all Employees.

Criteria	Nexthink Control
	ID-085: Secure Design and Application Threat Modeling Development teams receive feedback from architecture analysis, to ensure that the product is compliant with the Application Security Baseline.- Threat Modeling guideline- Definition of Ready (DoR)- Security Design Review – DoR
	ID-088: Security & Privacy Documentation Management The Policy Management Process describes how the documentation relevant to the Information Security Management System (ISMS) is governed, managed, maintained, and disseminated. Documents are re-viewed on a yearly basis following the Documentation Procedure.
	ID-090: Security & Privacy Roles and Responsibilities Security roles and responsibilities are defined and communicated for all personnel. Security governance policy and Acceptable usage policy defines roles and responsibilities.
	ID-091: Security Awareness & Trainings Nexthink provides its employee with mandatory initial and continuous security awareness training, aligned to the sensitivity of the data and systems they are required to perform their job duties.
	ID-092: Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem

Criteria	Nexthink Control
	ID-093: Security Objectives, Architecture and Design Nexthink documents its security architecture, including system and infrastructure security diagrams. Security principles and high-level security best practices are embedded in Nexthink's security strategy, and used as a reference when designing, implementing, and operating our Information Security Management System. Ensure during creation and review of Cloud Security policy and Engineering policy that these principles are present and updated if required.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**ID-008: Audit program** The organization performs manual testing and reviews of systems, accounts and controls as needed. The audit may be performed by internal teams or external auditors. The organization has defined auditing processes including system configuration monitoring, activity monitoring, access review, and controls compliance audit and results are reported to senior management. Metrics are defined to measure the effectiveness of controls and they are reported to/reviewed by senior management.
	ID-020: Code of Conduct and Acceptable Use of End-user Computing Acceptable use policy and code of Conduct is in place to guide the organization's personnel on the proper use of information assets and their roles and responsibilities. Ensure both policies are disseminated to all employees. Contracts include confidentiality clause.
	ID-024: Customer Audit and compliance report Request Ensure that customers have process to re-quest/receive audits and compliance reports and evidence.

Criteria	Nexthink Control
	ID-026: Data Breach Notification Nexthink documents and maintains a process to investigate suspected data breaches and duly notify affected parties in accordance with applicable law and regulations. This includes a data breach notification procedure and communication template and a data-breach specific procedure in the security incident response plan. The following procedures are available, approved and up to date: - Information Security Incident Response Plan - Personal Data Breach Notification
	ID-076: Privacy Terms and Consent Notices Ensure that the following requirements are duly documented and agreed by customers in the Contractual Agreements: - Privacy terms- Consents- Intended use- Notices- 3rd party Sub-processors
	ID-081: Responsible Disclosure Process Nexthink runs a responsible disclosure program where customers and external security researchers are encouraged to responsibly disclose any vulnerability to Nexthink about its infrastructure or products and provided with clear guidelines and communication channels.
	ID-092: Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem

Criteria	Nexthink Control
	ID-093: Security Objectives, Architecture and Design Nexthink documents its security architecture, including system and infrastructure security diagrams. Security principles and high-level security best practices are embedded in Nexthink's security strategy, and used as a reference when designing, implementing, and operating our Information Security Management System. Ensure during creation and review of Cloud Security policy and Engineering policy that these principles are present and updated if required.
	ID-102: Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.
	ID-113: Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.

4.1.3 CC3.0 - Common Criteria Related to Risk Assessment

Criteria	Nexthink Control
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**ID-022: Compliance Program Management** Compliance requirements of relevant legislative statutory, regulatory, and contractual controls are identified and implemented.
	ID-057: Management leadership Ensure business-oriented objectives and results are reported to the management. Committees are held as defined in the Security Governance policy.
	ID-083: Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
	ID-088: Security & Privacy Documentation Management The Policy Management Process describes how the documentation relevant to the Information Security Management System (ISMS) is governed, managed, maintained, and disseminated. Documents are re-viewed on a yearly basis following the Documentation Procedure.
	ID-089: Security & Privacy Governance Program Nexthink's security and privacy program maintains documentation of high-level policies and lower-level controls and procedures. The policies and procedures cover the design, development, implementation, operation, maintenance and monitoring of in-scope systems. Controls are developed and maintained following objectives, risk assessments, compliance, or customer requirements.
	ID-102: Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across	**ID-045: Free and Open-Source Software (FOSS) Security** Product dependencies (open or closed source) are scanned with a Software Component Analysis (SCA) tool looking for potential security vulnerabilities and licensing issues.

Criteria	Nexthink Control
the entity and analyzes risks as a basis for determining how the risks should be managed.	**ID-083: Risk Management Process** A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
	ID-085: Secure Design and Application Threat Modeling Development teams receive feedback from architecture analysis, to ensure that the product is compliant with the Application Security Baseline. - Threat Modeling guideline- Definition of Ready (DoR)- Security Design Review – DoR
	ID-102: Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.
	ID-113: Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.
	ID-116: Vulnerability and Patch Management Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure and across all systems managed by the IT team including servers and endpoints. Nexthink remediates security vulnerabilities based on their criticality and impact with a defined SLA.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**ID-083: Risk Management Process** A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
	ID-116: Vulnerability and Patch Management Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure and across all systems managed by the IT team including servers and endpoints. Nexthink remediates security vulnerabilities based on their criticality and impact with a defined SLA.

Criteria	Nexthink Control
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**ID-019: Change Management** Nexthink has defined a change management process defining the different type, approval workflow and review. System management tools are provisioned following the same requirements and configurations as any production system. - All changes must go through pull requests with code reviews. - Deployment happens in the same way as for the product components themselves, through build pipelines. - Cloud system management tools are developed according to the SDLC (including Definition of Ready and Definition of Done)
	ID-022: Compliance Program Management Compliance requirements of relevant legislative statutory, regulatory, and contractual controls are identified and implemented.
	ID-083: Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
	ID-085: Secure Design and Application Threat Modeling Development teams receive feedback from architecture analysis, to ensure that the product is compliant with the Application Security Baseline. - Threat Modeling guideline- Definition of Ready (DoR)- Security Design Review – DoR
	ID-102: Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.
	ID-113: Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.

4.1.4 CC4.0 - Common Criteria Related to Monitoring Activities

Criteria	Nexthink Control
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.	**ID-005: Application Security Testing** Application penetration tests are performed according to the defined Engineering Security policy.
	ID-008: Audit program The organization performs manual testing and reviews of systems, accounts and controls as needed. The audit may be performed by internal teams or external auditors. The organization has defined auditing processes including system configuration monitoring, activity monitoring, access review, and controls compliance audit and results are reported to senior management. Metrics are defined to measure the effectiveness of controls and they are reported to/reviewed by senior management.
	ID-009: Audit Related Training Education Awareness and Responsibilities Employees are informed and trained on the organization's monitoring and auditing process. Training is reviewed on a yearly basis or upon changes.
	ID-023: Configuration baselining and hardening Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.
	ID-052: Infrastructure Security Testing Penetration test are performed at least annually on Nexthink infrastructure or upon major changes. Vulnerabilities are identified and patch following the Vulnerability and patch management policy.
	ID-057: Management leadership Ensure business-oriented objectives and results are reported to the management. Committees are held as defined in the Security Governance policy.

Criteria	Nexthink Control
	ID-059: Metrics Measurements and Continuous Monitoring Metrics are defined to measure the effectiveness of controls and they are continuously monitored. KPIs are reviewed annually by the Security team to ensure accuracy and completeness.
	ID-081: Responsible Disclosure Process Nexthink runs a responsible disclosure program where customers and external security researchers are encouraged to responsibly disclose any vulnerability to Nexthink about its infrastructure or products and provided with clear guidelines and communication channels.
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.	**ID-008: Audit program** The organization performs manual testing and reviews of systems, accounts and controls as needed. The audit may be performed by internal teams or external auditors. The organization has defined auditing processes including system configuration monitoring, activity monitoring, access review, and controls compliance audit and results are reported to senior management. Metrics are defined to measure the effectiveness of controls and they are reported to/reviewed by senior management.
	ID-057: Management leadership Ensure business-oriented objectives and results are reported to the management. Committees are held as defined in the Security Governance policy.
	ID-059: Metrics Measurements and Continuous Monitoring Metrics are defined to measure the effectiveness of controls and they are continuously monitored. KPIs are reviewed annually by the Security team to ensure accuracy and completeness.
	ID-094: Security posture monitoring Nexthink continuously scans resources deployed in AWS accounts to ensure they are aligned with the AWS Services Secure Configuration Standard and deviations are reported and acted upon.

4.1.5 CC5.0 - Common Criteria Related to Control Activities

Criteria	Nexthink Control
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. **CC5.2** - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**ID-003: Access to Production Environment and Data** Nexthink implements tight access control and strong auditing mechanisms for employee access to production data of Nexthink Experience. Access to personal data is limited by least privileged. Access to production data on AWS is managed through AWS SSO connected to Nexthink Okta IdP and based on role-based access control limited to authorized personal. In addition, CloudTrail is enabled ensuring access to data is logged.
	ID-083: Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
	ID-077: Privileged Account Management (PAM) Nexthink defines policies and procedures to manage all privileged accounts by ensuring the principle of least privilege, mandatory Multi-Factor Authentication (MFA) and separation of privileges. Privileged accounts are reviewed on a periodic basis.
	ID-083: Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
	ID-084: Role-based access control (RBAC) Nexthink provisions access to systems following a role-based access control (RBAC) methodology, where employee access is based on their role.
	ID-093: Security Objectives, Architecture and Design Nexthink documents its security architecture, including system and infrastructure security diagrams. Security principles and high-level security best practices are embedded in Nexthink's security strategy, and used as a reference when designing, implementing, and operating our Information Security Management System. Ensure during creation and review of Cloud Security policy and Engineering policy that these principles are present and updated if required.

Criteria	Nexthink Control
	ID-100: Software Development Process Nexthink maintains a secure software development process, coding standards, and release strategy to ensure security is built-in to the products and applications. Cloud infrastructure changes and software code de-ploys follow a defined change request process with automated and/or manual reviews and approvals. Provisioning of any production system requires a change request that is reviewed and approved by engineering.
	ID-101: Source Code Management Nexthink stores its source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.
	ID-109: Tools Used for Auditing and Security Assessments Upon budgetary planning, the Security team reviews the existing and the needs for additional tooling or services.
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.	**ID-021: Competences** Nexthink provides employees the opportunity to attend conferences, access to training courses, studies to maintain and further advance their skills relevant to their job functions and business objectives.
	ID-051: Improvement process Identified control deficiencies are communicated to parties responsible for taking corrective action. Root cause analysis is performed, and remediation plans are proposed and monitored through resolution.
	ID-057: Management leadership Ensure business-oriented objectives and results are reported to the management. Committees are held as defined in the Security Governance policy.
	ID-083: Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
	ID-088: Security & Privacy Documentation Management

Criteria	Nexthink Control
	The Policy Management Process describes how the documentation relevant to the Information Security Management System (ISMS) is governed, managed, maintained, and disseminated. Documents are re-viewed on a yearly basis following the Documentation Procedure.
	ID-090: Security & Privacy Roles and Responsibilities Security roles and responsibilities are defined and communicated for all personnel. Security governance policy and Acceptable usage policy defines roles and responsibilities.
	ID-094: Security posture monitoring Nexthink continuously scans resources deployed in AWS accounts to ensure they are aligned with the AWS Services Secure Configuration Standard and deviations are reported and acted upon.
	ID-097: Shared Responsibility Model Nexthink has created a responsibility map based on the Software-as-a-Service model where the different areas of responsibility can be clearly identified.
	ID-113: Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.

4.1.6 CC6.0 - Common Criteria Related to Logical and Physical Access Controls

Criteria	Nexthink Control
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**ID-003: Access to Production Environment and Data** Nexthink implements tight access control and strong auditing mechanisms for employee access to production data of Nexthink Experience. Access to personal data is limited by least privileged. Access to production data on AWS is managed through AWS SSO connected to Nexthink Okta IdP and based on role-based access control limited to authorized personal. In addition, CloudTrail is enabled ensuring access to data is logged.
	ID-007: Asset management Nexthink inventories its assets within the information processing facility and ensures they have a clear owner so that they are accounted properly. IT maintains an asset inventory system for their in-scope assets. An annual review of the account owner is per-formed.
	ID-023: Configuration baselining and hardening Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.
	ID-028: Data Classification Ensure that the definition and classification level are in place for different datasets used. Ensure that the Confidentiality Policy contains the different relevant classification levels. Ensure that Engineering Security Policy supports the definition of data sets according to data classification. Ensure that the Cloud Security Policy contains data handling process including: - Encryption Requirements - Access Controls Ensure that the data retention policy sets retention requirements according to different datasets.

Criteria	Nexthink Control
	ID-031: Data Inventory and Lifecycle Management Data is classified according to its classification, and its lifecycle is defined. Transient and temporary data (or cache) is purged in a timely manner. The Data Classification and Data Inventory has been reviewed during the last year.
	ID-039: Encryption at Rest Nexthink protects endpoints data and confidential data by enforcing encryption on endpoints and removable storage devices. Nexthink customer data is encrypted at rest using industry-standard algorithms and key lengths.
	ID-042: Firewall Protection Nexthink implements network level protection for hosts and applications. Internal servers and applications are protected at the network level by the company's firewalls. Endpoints are protected at the network level by enabling the local firewall. Inbound Internet traffic and internal network traffic of Nexthink Experience is protected by virtual private cloud networking and security groups.
	ID-049: Identity and Access Management Ensure that right people, have access to right cloud access resources. This includes access to Azure. Access to right environments. Access to customer instances.
	ID-064: Network Management and Configuration Nexthink ensures that network layer security controls are in place to enable traffic filtering/monitoring for applicable environments.
	ID-069: Office Network and Wifi Access Office networks, including wireless access, are protected for internal business use only. Guest wireless access is provided on a separate logical network.
	ID-071: Password Policy Ensure that a password policy is defined implemented and enforced.
	ID-080: Protection of secret information Nexthink ensures that Nexthink Experience production keys and secrets are securely stored and protected

Criteria	Nexthink Control
	ID-095: Segregation of cloud environment Production, pre-production, testing, and development environments are segmented by dedicated AWS accounts. Deliverables must follow the change management process to change from one environment to another. Production environment is also designed to separate customer data in a hybrid single and multi-tenant architecture.
	ID-096: Service and Recovery Accounts Nexthink securely manages credentials of service accounts, which includes IP allow-listing and temporary credentials using the AWS Security Token Service. Recovery accounts are maintained to ensure emergency access to selected critical services.
	ID-098: Single Sign-On & Multi-Factor Authentication Nexthink implements single sign-on through Okta and Multi-Factor Authentication (MFA) to enable centralized management of identities and strong authentication. When technically possible, critical business applications must use an authentication system providing SSO capabilities based on Nexthink's centralized user directory.
	ID-101: Source Code Management Nexthink stores its source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.
	ID-115: VPN Remote Access Nexthink provides its employees with a secure VPN to access the corporate network remotely through an encrypted tunnel, using client-side TLS certificates and enforced multi-factor authentication based on MFA.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**ID-002: Access Establishment Modification and Termination** Nexthink's HR Operations and IT teams deprovision user access upon employees leaving the company. Nexthink new-hires on-boarding is coordinated between HR and IT to ensure appropriate access provisioning and system configurations are in place for each new hire. The HRIS system (BambooHR) sends automated notifications to the IT ServiceDesk prior to employee onboarding.

Criteria	Nexthink Control
	ID-080: Protection of secret information Nexthink ensures that Nexthink Experience production keys and secrets are securely stored and protected
	ID-082: Review of access rights User access permissions are reviewed as part of ongoing security monitoring as defined in the Access Control policy.
	ID-096: Service and Recovery Accounts Nexthink securely manages credentials of service accounts, which includes IP allow-listing and temporary credentials using the AWS Security Token Service. Recovery accounts are maintained to ensure emergency access to selected critical services.
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.	**ID-002: Access Establishment Modification and Termination** Nexthink's HR Operations and IT teams deprovision user access upon employees leaving the company. Nexthink new-hires on-boarding is coordinated between HR and IT to ensure appropriate access provisioning and system configurations are in place for each new hire. The HRIS system (BambooHR) sends automated notifications to the IT ServiceDesk prior to employee onboarding.
	ID-003: Access to Production Environment and Data Nexthink implements tight access control and strong auditing mechanisms for employee access to production data of Nexthink Experience. Access to personal data is limited by least privileged. Access to production data on AWS is managed through AWS SSO connected to Nexthink Okta IdP and based on role-based access control limited to authorized personal. In addition, CloudTrail is enabled ensuring access to data is logged.
	ID-011: AWS Accounts Provisioning process Nexthink provisions AWS accounts to grant access to required information systems and services through a documented and repeatable provisioning process to prevent poorly managed or incorrect access rights.

Criteria	Nexthink Control
	ID-029: Data Deletion Procedures - Data Retention Ensure that retention is enabled in the different components and technologies used in the Cloud Environment.
	ID-031: Data Inventory and Lifecycle Management Data is classified according to its classification, and its lifecycle is defined. Transient and temporary data (or cache) is purged in a timely manner. The Data Classification and Data Inventory has been reviewed during the last year.
	ID-082: Review of access rights User access permissions are reviewed as part of ongoing security monitoring as defined in the Access Control policy.
	ID-084: Role-based access control (RBAC) Nexthink provisions access to systems following a role-based access control (RBAC) methodology, where employee access is based on their role.
	ID-101: Source Code Management Nexthink stores its source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.	**ID-027: Data Center Security** Ensure server rooms and data centers comply with our policies and standards.
	ID-082: Review of access rights User access permissions are reviewed as part of ongoing security monitoring as defined in the Access Control policy.
	ID-002: Access Establishment Modification and Termination Nexthink's HR Operations and IT teams deprovision user access upon employees leaving the company. Nexthink new-hires on-boarding is coordinated between HR and IT to ensure appropriate access provisioning and system configurations are in place for each new hire. The HRIS system (BambooHR) sends automated notifications to the IT ServiceDesk prior to employee onboarding.

Criteria	Nexthink Control
	ID-075: Physical Security Controls Nexthink controls and restricts physical access to its offices. The workplace team keeps records of visitors. Offices are monitored for unauthorized access and protected against environmental hazards.
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.	**ID-029: Data Deletion Procedures - Data Retention** Ensure that retention is enabled in the different components and technologies used in the Cloud Environment.
	ID-031: Data Inventory and Lifecycle Management Data is classified according to its classification, and its lifecycle is defined. Transient and temporary data (or cache) is purged in a timely manner. The Data Classification and Data Inventory has been reviewed during the last year.
	ID-058: Media Disposal Process Nexthink ensures that media containing critical or sensitive data is disposed securely.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**ID-003: Access to Production Environment and Data** Nexthink implements tight access control and strong auditing mechanisms for employee access to production data of Nexthink Experience. Access to personal data is limited by least privileged. Access to production data on AWS is managed through AWS SSO connected to Nexthink Okta IdP and based on role-based access control limited to authorized personal. In addition, CloudTrail is enabled ensuring access to data is logged.
	ID-023: Configuration baselining and hardening Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.

Criteria	Nexthink Control
	ID-042: Firewall Protection Nexthink implements network level protection for hosts and applications. Internal servers and applications are protected at the network level by the company's firewalls. Endpoints are protected at the network level by enabling the local firewall. Inbound Internet traffic and internal network traffic of Nexthink Experience is protected by virtual private cloud networking and security groups.
	ID-049: Identity and Access Management Ensure that right people, have access to right cloud access resources. This includes access to Azure. Access to right environments. Access to customer instances.
	ID-063: Network Intrusion Detection Nexthink continuously analyze network traffic to identify potential malicious activity.Nexthink uses AWS GuardDuty to perform Network Intrusion Detection.
	ID-069: Office Network and Wifi Access Office networks, including wireless access, are protected for internal business use only. Guest wireless access is provided on a separate logical network.
	ID-080: Protection of secret information Nexthink ensures that Nexthink Experience production keys and secrets are securely stored and protected
	ID-095: Segregation of cloud environment Production, pre-production, testing, and development environments are segmented by dedicated AWS accounts. Deliverables must follow the change management process to change from one environment to another. Production environment is also designed to separate customer data in a hybrid single and multi-tenant architecture.
	ID-098: Single Sign-On & Multi-Factor Authentication Nexthink implements single sign-on through Okta and Multi-Factor Authentication (MFA) to enable centralized management of identities and strong authentication. When technically possible, critical business applications must use an authentication system providing SSO capabilities based on Nexthink's centralized user directory.

Criteria	Nexthink Control
	ID-101: Source Code Management Nexthink stores its source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.
	ID-115: VPN Remote Access Nexthink provides its employees with a secure VPN to access the corporate network remotely through an encrypted tunnel, using client-side TLS certificates and enforced multi-factor authentication based on MFA.
	ID-117: Web Application Firewall Nexthink implements web application firewall technology to protects web resources from malicious attacks.
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.	**ID-003: Access to Production Environment and Data** Nexthink implements tight access control and strong auditing mechanisms for employee access to production data of Nexthink Experience. Access to personal data is limited by least privileged. Access to production data on AWS is managed through AWS SSO connected to Nexthink Okta IdP and based on role-based access control limited to authorized personal. In addition, CloudTrail is enabled ensuring access to data is logged.
	ID-023: Configuration baselining and hardening Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.

Criteria	Nexthink Control
	ID-028: Data Classification Ensure that the definition and classification level are in place for different datasets used. Ensure that the Confidentiality Policy contains the different relevant classification levels. Ensure that Engineering Security Policy supports the definition of data sets according to data classification. Ensure that the Cloud Security Policy contains data handling process including: - Encryption Requirements - Access Controls Ensure that the data retention policy sets retention requirements according to different datasets.
	ID-039: Encryption at Rest Nexthink protects endpoints data and confidential data by enforcing encryption on endpoints and removable storage devices. Nexthink customer data is encrypted at rest using industry-standard algorithms and key lengths.
	ID-040: Encryption in transit (in motion) Nexthink encrypts customer data in transit using industry-standard technologies such as TLS 1.2, both for traffic from public networks and for internal network traffic. All customer data transmitted between AWS services, and between the Internet and AWS services is encrypted in transit.
	ID-064: Network Management and Configuration Nexthink ensures that network layer security controls are in place to enable traffic filtering/monitoring for applicable environments.
	ID-086: Secure File Sharing Exchange of sensitive information with customers is performed via secure file transfer which implements end-to-end encryption.
	ID-094: Security posture monitoring Nexthink continuously scans resources deployed in AWS accounts to ensure they are aligned with the AWS Services Secure Configuration Standard and deviations are reported and acted upon.

Criteria	Nexthink Control
	ID-095: Segregation of cloud environment Production, pre-production, testing, and development environments are segmented by dedicated AWS accounts. Deliverables must follow the change management process to change from one environment to another. Production environment is also designed to separate customer data in a hybrid single and multi-tenant architecture.
	ID-115: VPN Remote Access Nexthink provides its employees with a secure VPN to access the corporate network remotely through an encrypted tunnel, using client-side TLS certificates and enforced multi-factor authentication based on MFA.
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.	**ID-023: Configuration baselining and hardening** Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.
	ID-056: Malware Protection Nexthink protects endpoint devices by installing an EDR agent. Endpoint devices are enrolled in a Mobile Device Management solution such as JamF or Intune which will install the malware protection agent. Nexthink analysis and monitors endpoints for malicious activity including network and host activity.
	ID-101: Source Code Management Nexthink stores its source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.

Criteria	Nexthink Control
	ID-112: User Endpoint Security Controls and Configuration Nexthink maintains security configurations across endpoints using Mobile Device Management systems. Nexthink implements restrictions to ensure that access to production environments is restricted to company managed devices. Nexthink denies by policy the usage of devices that are not managed or owned by the company (BYOD).

4.1.7 CC7.0 - Common Criteria Related to Systems Operations

Criteria	Nexthink Control
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.	**ID-018: Centralized Security Information and Event Management** The Information Security Policy and the Cloud Security policy describe the information required to be captured in logs. Security-relevant logs are generated both at the cloud provider level and at the application level, ensuring security-relevant events are logged and centralized to ensure they can be efficiently queried and cannot be tampered with, including antivirus logs, AWS CloudTrail, Azure audit logs, and application-level security events.
	ID-023: Configuration baselining and hardening Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.
	ID-045: Free and Open-Source Software (FOSS) Security Product dependencies (open or closed source) are scanned with a Software Component Analysis (SCA) tool looking for potential security vulnerabilities and licensing issues.
	ID-052: Infrastructure Security Testing Penetration tests are performed at least annually on Nexthink infrastructure or upon major changes. Vulnerabilities are identified and patch following the Vulnerability and patch management policy.
	ID-081: Responsible Disclosure Process Nexthink runs a responsible disclosure program where customers and external security researchers are encouraged to responsibly disclose any vulnerability to Nexthink about its infrastructure or products and provided with clear guidelines and communication channels.
	ID-094: Security posture monitoring Nexthink continuously scans resources deployed in AWS accounts to ensure they are aligned with the AWS Services Secure Configuration Standard and deviations are reported and acted upon.

Criteria	Nexthink Control
	ID-116: Vulnerability and Patch Management Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure and across all systems managed by the IT team including servers and endpoints. Nexthink remediates security vulnerabilities based on their criticality and impact with a defined SLA.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	**ID-018: Centralized Security Information and Event Management** The Information Security Policy and the Cloud Security policy describe the information required to be captured in logs. Security-relevant logs are generated both at the cloud provider level and at the application level, ensuring security-relevant events are logged and centralized to ensure they can be efficiently queried and cannot be tampered with, including antivirus logs, AWS CloudTrail, Azure audit logs, and application-level security events.
	ID-061: Monitoring and Capacity Management Monitoring of critical components is implemented, capacity and sizing procedures.
	ID-094: Security posture monitoring Nexthink continuously scans resources deployed in AWS accounts to ensure they are aligned with the AWS Services Secure Configuration Standard and deviations are reported and acted upon.
	ID-106: Threat Intelligence Monitoring Stay up to date with the latest threat intel news related to threats and security risks that might impact Nexthink. The Security Team subscribes to news, feeds, forums, and special interest groups to receive updates on threat-intelligence and updates on applicable regulations and compliance.

Criteria	Nexthink Control
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.	**ID-018: Centralized Security Information and Event Management** The Information Security Policy and the Cloud Security policy describe the information required to be captured in logs. Security-relevant logs are generated both at the cloud provider level and at the application level, ensuring security-relevant events are logged and centralized to ensure they can be efficiently queried and cannot be tampered with, including antivirus logs, AWS CloudTrail, Azure audit logs, and application-level security events.
	ID-092: Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem
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.	**ID-026: Data Breach Notification** Nexthink documents and maintains a process to investigate suspected data breaches and duly notify affected parties in accordance with applicable law and regulations. This includes a data breach notification procedure and communication template and a data-breach specific procedure in the security incident response plan. The following procedures are available, approved and up to date: - Information Security Incident Response Plan - Personal Data Breach Notification
	ID-065: Non-Compliance Investigation, Sanctions and Disciplinary process Ensure that a disciplinary process is implemented and applied according to the company policy.

Criteria	Nexthink Control
	ID-092: Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem
	ID-116: Vulnerability and Patch Management Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure and across all systems managed by the IT team including servers and endpoints. Nexthink remediates security vulnerabilities based on their criticality and impact with a defined SLA.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	**ID-016: Business Continuity and Disaster Recovery Test Plan** Test exercises are performed according to policy.
	ID-026: Data Breach Notification Nexthink documents and maintains a process to investigate suspected data breaches and duly notify affected parties in accordance with applicable law and regulations. This includes a data breach notification procedure and communication template and a data-breach specific procedure in the security incident response plan. The following procedures are available, approved and up to date: - Information Security Incident Response Plan - Personal Data Breach Notification
	ID-051: Improvement process

Criteria	Nexthink Control
	Identified control deficiencies are communicated to parties responsible for taking corrective action. Root cause analysis is performed, and remediation plans are proposed and monitored through resolution.
	ID-092: Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem
	ID-102: Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.

4.1.8 CC8.0 - Common Criteria Related to Change Management

Criteria	Nexthink Control
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**ID-005: Application Security Testing** Application penetration tests are performed according to the defined Engineering Security policy.
	ID-011: AWS Accounts Provisioning process Nexthink provisions AWS accounts to grant access to required information systems and services through a documented and repeatable provisioning process to prevent poorly managed or incorrect access rights.
	ID-019: Change Management Nexthink has defined a change management process defining the different type, approval workflow and review. System management tools are provisioned following the same requirements and configurations as any production system. - All changes must go through pull requests with code reviews. - Deployment happens in the same way as for the product components themselves, through build pipelines. - Cloud system management tools are developed according to the SDLC (including Definition of Ready and Definition of Done)
	ID-023: Configuration baselining and hardening Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.

Criteria	Nexthink Control
	ID-036: Emergency changes An emergency change process is in place. Details of any emergency change are retroactively documented and approved. Emergency changes are covered via: - The Internal bugs process for the SDLC and Cloud Platform - The high impact changes for CloudOps. - The emergency changes for IT Corporate.
	ID-085: Secure Design and Application Threat Modeling Development teams receive feedback from architecture analysis, to ensure that the product is compliant with the Application Security Baseline.- Threat Modeling guideline-Definition of Ready (DoR)- Security Design Review – DoR
	ID-092: Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem

Criteria	Nexthink Control
	ID-093: Security Objectives, Architecture and Design Nexthink documents its security architecture, including system and infrastructure security diagrams. Security principles and high-level security best practices are embedded in Nexthink's security strategy, and used as a reference when designing, implementing, and operating our Information Security Management System. Ensure during creation and review of Cloud Security policy and Engineering policy that these principles are present and updated if required.
	ID-100: Software Development Process Nexthink maintains a secure software development process, coding standards, and release strategy to ensure security is built-in to the products and applications. Cloud infrastructure changes and software code de-ploys follow a defined change request process with automated and/or manual reviews and approvals. Provisioning of any production system requires a change request that is reviewed and approved by engineering.
	ID-101: Source Code Management Nexthink stores its source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.
	ID-116: Vulnerability and Patch Management Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure and across all systems managed by the IT team including servers and endpoints. Nexthink remediates security vulnerabilities based on their criticality and impact with a defined SLA.

4.1.9 CC9.0 - Common Criteria Related to Risk Mitigation

Criteria	Nexthink Control
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**ID-025: Cyber Liability Insurance** Ensure appropriate insurance coverage for the identified liabilities based on the identified risks. Insurance coverage is revised on a yearly basis.
	ID-083: Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	**ID-041: External consultant management** Nexthink manages lifecycle of external consultants, and ensures they acknowledge organizational policies before getting access to company resources.
	ID-113: Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.

4.1.10 Additional Criteria for Availability

Criteria	Nexthink Control
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.	**ID-061: Monitoring and Capacity Management** Monitoring of critical components is implemented, capacity and sizing procedures.
	ID-100: Software Development Process Nexthink maintains a secure software development process, coding standards, and release strategy to ensure security is built-in to the products and applications. Cloud infrastructure changes and software code de-ploys follow a defined change request process with automated and/or manual reviews and approvals. Provisioning of any production system requires a change request that is reviewed and approved by engineering.
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.	**ID-015: Business Continuity and Disaster Recovery** BCDR plan are defined and reviewed annually or upon major changes.
	ID-027: Data Center Security Ensure server rooms and data centers comply with our policies and standards.
	ID-061: Monitoring and Capacity Management Monitoring of critical components is implemented, capacity and sizing procedures.
	ID-092: Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem

Criteria	Nexthink Control
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.	**ID-016: Business Continuity and Disaster Recovery Test Plan** Test exercises are performed according to policy.

4.2 Part B: Nexthink Control Activities Provided by Nexthink and Tests Performed and Results provided by EY

Control Activity	Tests Performed	Test Results
ID-002 - Access Establishment Modification and Termination Nexthink's HR Operations and IT teams deprovision user access upon employees leaving the company. Nexthink new-hires on-boarding is coordinated between HR and IT to ensure appropriate access provisioning and system configurations are in place for each new hire. The HRIS system (BambooHR) sends automated notifications to the IT ServiceDesk prior to employee onboarding. Nexthink follows a least privilege model based on RBAC applied for onboarding as well as role and access changes.	• Inspected the access control policy and noted that there were defined processes for provisioning, modification, and termination of user access. • Inspected a sample of new joiners to determine whether access was provisioned as described in the matrix of roles per job function. • Inspected evidence of the configuration to enforce approvals for the provisioning of engineering access and noted that the configuration was available for the full duration of the audit period. • Inspected a sample of non-engineering employees with a modification in their role / function to determine whether the access was modified in line with the requirements of list of roles per job function. • Inspected a sample of leavers to determine whether logical access had been disabled and whether IT equipment had been retrieved as the employee left the company.	Exceptions noted: EY noted for 1 out of 12 samples the new user received one additional permission that was not defined for the job position. Further, gained the understanding that the client identified the exception through internal detective controls and applied corrective actions. **No further exceptions noted**

Control Activity	Tests Performed	Test Results
ID-003 - Access to Production Environment and Data Nexthink implements tight access control and strong auditing mechanisms for employee access to production data of Nexthink Experience. Access to personal data is limited by least privileged. Access to production data on AWS is managed through AWS SSO connected to Nexthink Okta IdP and based on role-based access control limited to authorized personal. In addition, CloudTrail is enabled ensuring access to data is logged.	• Inspected evidence to determine whether SSO was enabled for AWS through Okta. • Inspected the configuration to determine whether the automated control was implemented and was not changed during the audit period. • Inspected the annual review of AWS accounts. • Inspected evidence that CloudTrail was enabled and records account activity across the AWS infrastructure. • Inspected evidence to determine whether the logs from AWS were transferred to a centralized event management tool to facilitate the monitoring and prevent the tampering of audit logs.	No exception noted
ID-005 - Application Security Testing Application penetration tests are performed according to the defined Engineering Security policy.	• Inspected the content of the Engineering Security Policy to determine whether penetration testing must be performed at least annually by external parties. • Inspected evidence to determine whether a third-party had been contracted during the audit period to perform a penetration test on the product. • Inspected investigations, which were performed to conduct an internal assessment of the vulnerabilities identified by the third-party.	No exception noted

Control Activity	Tests Performed	Test Results
ID-007 - Asset management Nexthink inventories its assets within the information processing facility and ensures they have a clear owner so that they are accounted properly. IT maintains an asset inventory system for their in-scope assets. An annual review of the account owner is performed.	• Inspected evidence to determined that the review of active AWS accounts was performed. • Inspected evidence to determine whether the review of the IT infrastructure assets was performed during the 6-month audit period. • Inspected evidence to determine whether the review of the automated provisioning of VMs was performed during the 6-month period.	No exception noted
ID-008 - Audit program The organization performs manual testing and reviews of systems, accounts and controls as needed. The audit may be performed by internal teams or external auditors. The organization has defined auditing processes including system configuration monitoring, activity monitoring, access review, and controls compliance audit and results are reported to senior management. Metrics are defined to measure the effectiveness of controls and they are reported to/reviewed by senior management.	• Inspected evidence to determine whether an audit plan exists which defines the scope and resources of the audits to be conducted and that external parties had been engaged to perform internal and external audits. • Inspected evidence to determine whether internal KPIs were defined and monitored to measure the performance of metrics that were considered to be relevant to the information security function. • Inspected evidence to determine whether the scope of the indicators that were monitored has been reviewed by the security function during the audit period. • Inspected evidence that the information security roadmap and audit program, as well as the measurement results from KPIs had been presented to senior management during the audit period.	No exception noted

Control Activity	Tests Performed	Test Results
ID-009 - Audit Related Training Education Awareness and Responsibilities Employees are informed and trained on the organization's monitoring and auditing process. Training is reviewed on a yearly basis or upon changes.	• Inspected evidence to determine whether training materials were updated during the audit period and distributed to the relevant employees to inform them about the organization's auditing processes.	No exception noted
ID-011 - AWS Accounts Provisioning process Nexthink provisions AWS accounts to grant access to required information systems and services through a documented and repeatable provisioning process to prevent poorly managed or incorrect access rights.	• Inspection a sample to determine whether account creation requests were approved, and the provisioning was reviewed via approval of pull-requests.	No exception noted

Control Activity	Tests Performed	Test Results
ID-012 - Background Check Reviews Nexthink employees undergo systematic background screening prior to employment. The checks performed are aligned to the risk associated to the job position. Background checks are performed by the third-party HireRight.	• Inspected internal procedures to determine whether background checks must be performed for all new hires. • Inspected a sample of new hires for determining that background checks were performed.	Exceptions noted: EY noted for 3 out of 12 samples not enough evidence could be provided to determine whether a background check was performed. Furthermore, EY noted for 1 out of 12 samples the background check verification was not requested. **No further exceptions noted**
ID-014 - Board of directors A Board Charter outlines the roles, responsibilities, and authorities of the Board of Directors (individually and collectively).	• Inspected evidence to determine whether the rules governing the organization and responsibilities of the Board of Directors were documented in the Board Charter that was part of the Shareholder's Agreement. • Inspected a copy of the Shareholder's Agreement to determine whether the document had been signed in January 2021. Determined that there have been no changes to the document since January 2021.	No exception noted

Control Activity	Tests Performed	Test Results
ID-015 - Business Continuity and Disaster Recovery BCDR plan are defined and reviewed annually or upon major changes.	• Inspected the content of the Business Continuity Disaster Recovery Plan Procedure to determine whether requirements were in place for performing business impact analyses and documenting and testing recovery activities. • Inspected the evidence to determine whether the plan had been reviewed during the audit period. • Determined that dedicated plans and strategies were documented to support the continuity of operations and services of the corporate IT infrastructure and the cloud environment in the event of a disruption. Based on inspection of the documents for the IT disaster recovery plan and the Cloud disaster recovery and BCP plan, determined that the documents had been reviewed during the audit period.	No exception noted

Control Activity	Tests Performed	Test Results
ID-016 - Business Continuity and Disaster Recovery Test Plan Test exercises are performed according to policy.	• Inspected the content of the Business Continuity Disaster Recovery Plan Procedure to determine whether requirements were in place for performing business impact analyses and documenting and testing recovery activities. • Inspected a random sample of relevant BCP scenarios identified for Cloud and IT infrastructure to determine whether test exercises had been performed.	Exceptions noted: EY noted for 3 out of 5 samples not enough evidence could be provided to confirm that test objectives were defined and that end-to-end tests were performed to validate the full scope of recovery activities. **No further exceptions noted**

Control Activity	Tests Performed	Test Results
ID-018 - Centralized Security Information and Event Management The Information Security Policy and the Cloud Security policy describe the information required to be captured in logs. Security-relevant logs are generated both at the cloud provider level and at the application level, ensuring security-relevant events are logged and centralized to ensure they can be efficiently queried and cannot be tampered with, including antivirus logs, AWS CloudTrail, Azure audit logs, and application-level security events.	• Inspected the content of the Information Security Policy and the Cloud Security Policy to determine whether requirements were defined for capturing audit logs and collecting relevant audit logs in a central tool. • Inspected internal documentation to determine whether relevant data sources, including the cloud provider, have been identified to determine whether the audit logs from the identified sources were transferred to a central tool, Splunk, to facilitate the administration of audit logs. • Inspected evidence from Splunk to determine whether retention periods and integrity checks were configured for the audit logs of the data sources defined as relevant. • Inspected the Splunk logs and noted that audit events had been ingested from the different data sources for the full duration of the audit period.	No exception noted

Control Activity	Tests Performed	Test Results
ID-019 - Change Management Nexthink has defined a change management process defining the different type, approval workflow and review. System management tools are provisioned following the same requirements and configurations as any production system. - All changes must go through pull requests with code reviews. - Deployment happens in the same way as for the product components themselves, through build pipe-lines. - Cloud system management tools are developed according to the SDLC (including Definition of Ready and Definition of Done).	• Inspected a random sample of regular and standard changes to determine whether: ○ Standard changes were applied based on the defined schedule and were based on pre-approved templates ○ Regular changes were approved as per the requirements defined in the change management procedure for IT infrastructure • Inspected a random sample of releases of the Nexthink product to determine whether changes were applied in line with the requirements of the processes defined.	Exceptions noted: EY noted for 5 out of 5 samples the changes did not follow the defined change process. In particular 2 changes were not formally tested, in addition, no comprehensive evidence was available to determine whether 4 changes were approved by appropriate persons. **No further exceptions noted**
ID-020 - Code of Conduct and Acceptable Use of End-user Computing Acceptable use policy and code of Conduct is in place to guide the organization's personnel on the proper use of information assets and their roles and responsibilities. Ensure both policies are disseminated to all employees. Contracts include confidentiality clause.	• Inspected evidence to determine whether an Acceptable Use Policy and a Code of Conduct were in place. • Inspected a random sample of new hires to determine whether ○ New joiners confirmed their acknowledgement of the Code of Conduct and Acceptable Usage Policy by signing the policy acceptance form ○ New joiners contracts contain a confidentiality clause.	No exception noted

Control Activity	Tests Performed	Test Results
ID-022 - Compliance Program Management Compliance requirements of relevant legislative statutory, regulatory, and contractual controls are identified and implemented.	• Inspected evidence and determine that the specific roles and responsibilities were defined in the Security Governance Policy. • Inspected the policy to determine whether certain committees were defined where the legal team participates to provide updates and discuss changes in the regulatory environment. • Inspected a random sample of security committee meetings to determine whether the meetings were held within the frequency defined in the Security Governance Policy.	No exception noted
ID-023 - Configuration baselining and hardening Nexthink provisions systems using infrastructure as code and pre-approved configuration as well as a golden image approved by the security team in order to reduce the attack surface. The hardening of the Nexthink Appliance is based on the CIS CentOS 7 L1 2.2.0 standard and is enforced through the nxhardening and nxcloud components for every release.	• Inspected evidence to determine whether the security policies for IT infrastructure and appliances exist as infrastructure as code and that changes to the security policies were subject to pull request approvals. • Inspected a sample of the integrity checks from the standard change plan schedule to determine whether checks were performed to verify that the configuration provisioning of the IT infrastructure was performed as expected. • Inspected an assessment performed during the audit period and noted that the results confirmed that Nexthink's appliances were hardened.	No exception noted
ID-025 - Cyber Liability Insurance Ensure appropriate insurance coverage for the identified liabilities based on the identified risks. Insurance coverage is revised on a yearly basis.	• Inspected the insurance certificates for cyber and data protection coverage to determine whether appropriate coverage was available during the audit period.	No exception noted

Control Activity	Tests Performed	Test Results
ID-026 - Data Breach Notification Nexthink documents and maintains a process to investigate suspected data breaches and duly notify affected parties in accordance with applicable law and regulations. This includes a data breach notification procedure and communication template and a data-breach specific procedure in the security incident response plan. The following procedures are available, approved and up to date: - Information Security Incident Response Plan - Personal Data Breach Notification.	• Inspected evidence to determine whether the following documents were approved and have been reviewed during the audit period: ○ Nexthink - Information Security Incident Response Plan ○ Nexthink - Personal Data Breach Notification Procedure ○ Nexthink - Information Security Incident Communication Procedure • Determined that there have been no data breach events during the audit period.	No occurrence of the control
ID-027 - Data Center Security Ensure server rooms and data centers comply with our policies and standards.	• Inspected evidence to determine whether a review of users who have access to the data center facilities was performed in 2022 by the IT Infrastructure Manager. • Inspected evidence for a sample of 25 randomly selected IT infrastructure changes to determine whether the changes were approved as required in the control procedure.	No exception noted

Control Activity	Tests Performed	Test Results
ID-028 - Data Classification Ensure that the definition and classification level are in place for different datasets used. Ensure that the Confidentiality Policy contains the different relevant classification levels. Ensure that Engineering Security Policy supports the definition of data sets according to data classification. Ensure that the Cloud Security Policy contains data handling process including: - Encryption Requirements - Access Controls Ensure that the data retention policy sets retention requirements according to different datasets.	• Inspected the content of the following internal documents to determine whether classification levels for different datasets were defined: ○ Asset classification policy ○ Confidentiality policy ○ Confidentiality guidelines ○ Engineering security policy ○ Cloud security policy ○ Data retention policy • Determined that guidelines for handling, retaining, and disposing data, based on classification, were defined. • Determined that the principles for access controls and protection of data according to its classification were embedded in the security policies.	No occurrence of the control
ID-029 - Data Deletion Procedures - Data Retention Ensure that retention is enabled in the different components and technologies used in the Cloud Environment.	• Inspected a random sample of AWS backup buckets to determine whether retention was enabled. with the requirements of the Data Retention Policy.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-031 - Data Inventory and Lifecycle Management Data is classified according to its classification, and its lifecycle is defined. Transient and temporary data (or cache) is purged in a timely manner. The Data Classification and Data Inventory has been reviewed during the last year.	• Inspected evidence to determine whether a Data Classification Procedure was in place describing the classification types considered within the company and requirements for protection of confidential and personal data. • Inspected the content of the "data inventory document" to determine whether the inventory summarized the data types contained in the Nexthink Experience product and identified the classification for each data type. • Determined that the document had been reviewed during the audit period. • Inspected evidence to determine whether Transient and temporary data (or cache) was purged in a timely manner.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-036 - Emergency changes An emergency change process is in place. Details of any emergency change are retroactively documented and approved. Emergency changes are covered via: - The Internal bugs process for the SDLC and Cloud Platform - The high impact changes for CloudOps. - The emergency changes for IT Corporate.	• Inspected a sample of emergency changes implemented in the corporate IT infrastructure to determine whether the changes were retroactively reviewed as described in the process description for emergency changes for IT corporate. • Inspected a random sample of emergency changes implemented in the cloud platform to determine whether the changes have been tested.	Exceptions noted: EY noted for 3 out of 8 samples of cloud platform emergency changes the evidence of test results were not documented. EY that for 5 out of 5 samples the approval from the Cloud Operations Manager was not available. EY noted the process of approval of infrastructure maintenance releases was not in place during the report period. **No further exceptions noted**
ID-037 - Employee Incentives and Rewards Employees receive regular peer recognition, feed-back and rewards for positive behavior and impact.	• Inspected evidence to determine whether a program was defined for identifying and rewarding the highest performing and most impactful employees. • Inspected evidence to determine whether a monitoring was in place to evaluate reward levels for different performance categories.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-038 - Employee performance review process Ensure that a formal process to measure employee performance is implemented.	• Inspected evidence to determine whether an employee performance review campaign was conducted during the audit period.	No exceptions noted
ID-039 - Encryption at Rest Nexthink protects endpoints data and confidential data by enforcing encryption on endpoints and removable storage devices. Nexthink customer data is encrypted at rest using industry-standard algorithms and key lengths.	• Inspected evidence to determine whether security policies were enabled through MDM solutions to enforce data encryption on endpoints and removable storage devices. • Inspected evidence of the configuration of the backup tool to determine whether backup file encryption was enabled. • Inspected evidence to determine whether reviews of privileged accounts were performed during the audit period.	No exceptions noted
ID-040 - Encryption in transit (in motion) Nexthink encrypts customer data in transit using industry-standard technologies such as TLS 1.2, both for traffic from public networks and for internal network traffic. All customer data transmitted between AWS services, and between the Internet and AWS services is encrypted in transit.	• Inspected evidence of the existing security configuration in the Cloud environment to determine whether TLS 1.2 security policies were enabled to ensure the encryption of customer data transmitted between AWS services. • Inspected the result of a product vulnerability report to determine whether the host supports the TLS 1.2 to ensure the protection of data traffic between the application and the network.	No exceptions noted
ID-041 - External consultant management Nexthink manages lifecycle of external consultants, and ensures they acknowledge organizational policies before getting access to company resources.	• Inspected a sample of external consultants to determine whether the selected consultants had acknowledged the required policies.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-042 - Firewall Protection Nexthink implements network level protection for hosts and applications. Internal servers and applications are protected at the network level by the company's firewalls. Endpoints are protected at the network level by enabling the local firewall. Inbound Internet traffic and internal network traffic of Nexthink Experience is protected by virtual private cloud networking and security groups.	• Inspected documentation of the network architecture and network segmentation to determine whether internal servers and applications were protected by the company's firewalls. • Inspected evidence to determine that the company maintains an inventory of the firewalls and that monitoring solutions were available to support network security management. • Inspected a random sample of IT infrastructure changes to determine whether the changes were approved as required in the control procedure. • Inspected evidence to determine whether Mobile Device Management solutions were in place and that firewall security policies were enabled for company-managed devices.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-045 - Free and Open-Source Software (FOSS) Security Product dependencies (open or closed source) are scanned with a Software Component Analysis (SCA) tool looking for potential security vulnerabilities and licensing issues.	• Inspected evidence to determine whether requirements were defined for performing code analysis for identifying vulnerabilities on third-party and open-source software components. • Inspected a random sample of development tasks to determine whether software component analysis had been performed.	Exceptions noted: EY noted for 7 out of 25 samples the result of the software component analysis scan was not available, therefore, the test could not be performed for the selected samples. **No further exceptions noted**
ID-047 - HR Management and Reporting HR maintains an inventory of job descriptions defined and duly approved and accepted by employees.	• Inspected evidence to determine whether job descriptions were maintained in the HR system. • Inspected a random sample of access provisioning for new users to determine whether job responsibilities were duly accepted by employees.	No exceptions noted
ID-049 - Identity and Access Management Ensure that right people, have access to right cloud access resources. This includes access to Azure. Access to right environments. Access to customer instances.	• Inspected policies of provisioning of temporary access to AWS production accounts to determine whether requests had to be approved and access was granted only for a limited period. • Inspected a random sample of new AWS access created to determine whether access was appropriately approved and granted for a limited period.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-051 - Improvement process Identified control deficiencies are communicated to parties responsible for taking corrective action. Root cause analysis is performed, and remediation plans are proposed and monitored through resolution.	• Inspected a random sample of non-conformities to determine that: ○ Non-conformities were registered in the GRC tool and were assigned to a responsible person with a specified due date. ○ Root cause analyses were performed and documented for the identified non-conformities. ○ Remediation plans were documented for the identified non-conformities with defined deadlines.	No exceptions noted
ID-052 - Infrastructure Security Testing Penetration test are performed at least annually on Nexthink infrastructure or upon major changes. Vulnerabilities are identified and patch following the Vulnerability and patch management policy.	• Inspected evidence to determine whether a penetration test had been performed in the last year and that the results were reported. • Inspected a random sample of vulnerabilities identified during penetration tests to determine whether vulnerabilities were resolved in line with the requirements of the vulnerability management policy.	No exceptions noted
ID-053 - Internal Business Communications Ensure that formal communication channels are defined and communicated to all Employees.	• Inspected evidence of activity in the company's internal community to determine whether a channel was available to reach out to all employees for communicating changes or relevant information about the organization. • Inspected for a random sample of monthly dates to determine whether company video conferences had been held as per the defined frequency.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-056 - Malware Protection Nexthink protects endpoint devices by installing an EDR agent. Endpoint devices are enrolled in a Mobile Device Management solution such as JamF or Intune which will install the malware protection agent. Nexthink analysis and monitors endpoints for malicious activity including network and host activity.	• Inspected evidence to determine whether security policies for endpoint protection were managed by mobile device management solutions. • Inspected evidence from Cortex XDR to determine whether prevention rules and profiles were set up. • Inspected for a random sample of incidents raised in Cortex XDR whether an investigation took place.	No exceptions noted
ID-057 - Management leadership Ensure business-oriented objectives and results are reported to the management. Committees are held as defined in the Security Governance policy.	• Inspected evidence for a random sample of committee meetings to determine whether the committees held meetings as per the frequency defined in the Security Governance Policy.	No exceptions noted
ID-058 - Media Disposal Process Nexthink ensures that media containing critical or sensitive data is disposed securely.	• Inspected evidence to determine the media disposal was executed appropriately for Lausanne. • Determined there were no additional occurrences of media disposal during the audit period for Lausanne. • Determined there were no occurrences of the control during the audit period for the sites in Boston and Madrid.	No exceptions noted
ID-059 - Metrics Measurements and Continuous Monitoring Metrics are defined to measure the effectiveness of controls and they are continuously monitored. KPIs are reviewed annually by the Security team to ensure accuracy and completeness.	• Inspected evidence of internal metrics and key performance indicators (KPIs) to determine that the list of indicators had been reviewed. • Inspected evidence of the semi-annual ISMS & PIMS Steering Committee Meetings to determine the meetings were performed and follow up on KPI report was part of the meeting agenda.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-061 - Monitoring and Capacity Management Monitoring and Capacity Management.	• Inspected a random sample of the defined alerts to determine whether the alert rules were implemented in the monitoring tool. • Inspected evidence to determine whether a capacity forecast was prepared for 2022. • Inspected a random sample of IT infrastructure capacity alerts to determine whether the alerts were resolved. • Inspected evidence of the bi-annual capacity planning review to determine whether the review was performed.	No exceptions noted
ID-063 - Network Intrusion Detection Nexthink continuously analyze network traffic to identify potential malicious activity. Nexthink uses AWS GuardDuty to perform Network Intrusion Detection.	• Determined that GuardDuty was enabled in AWS to monitor accounts for malicious activity. • Inspected a random sample of alerts from Mnemonic and to determine whether identified issues were analyzed and followed up with.	No exceptions noted
ID-064 - Network Management and Configuration Nexthink ensures that network layer security controls are in place to enable traffic filtering/monitoring for applicable environments.	• Inspected documentation of the network architecture and network segmentation to determine whether internal servers and applications were protected by the company's firewalls. • Determined the company maintains an inventory of the firewalls and that monitoring solutions were available to support network security management. • Inspected a random sample of IT infrastructure changes to determine whether the changes were approved as required in the control procedure. • Inspected evidence to determine whether Mobile Device Management solutions were in place and that firewall security policies were enabled for company-managed devices.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-065 - Non-Compliance Investigation, Sanctions and Disciplinary process Ensure that a disciplinary process is implemented and applied according to the company policy.	• Inspected the Information Security Disciplinary Procedure to determine whether a process and responsibilities for addressing non compliances or policy violations was defined.	No occurrence of the control
ID-069 - Office Network and Wifi Access Office networks, including wireless access, are protected for internal business use only. Guest wireless access is provided on a separate logical network.	• Inspected the configuration of guest access for the locations in scope (Boston, Lausanne, Madrid) to determine whether corporate networks were segregated from external or guest access. • Inspected evidence to determine whether a review of the network segmentation for the locations in scope was performed during the audit period.	No exceptions noted
ID-071 - Password Policy Ensure that a password policy is defined implemented and enforced.	• Inspected the content of the password policy to determine whether requirements were defined for the password configuration of normal users and high privileged users. • Inspected evidence of the configuration of password settings for normal and high privileged user accounts to determine whether the settings were defined as per the policy.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-075 - Physical Security Controls Nexthink controls and restricts physical access to its offices. The workplace team keeps records of visitors. Offices are monitored for unauthorized access and protected against environmental hazards.	• Performed virtual inspections of the sites in scope (Boston, Madrid and Lausanne) to determine the following: ○ Office access points were protected by badge controls. Digital records were available about the use of badges, entry points and time of access ○ Access points were monitored by CCTV. CCTV recording was motion activated and the logs were kept for a period of at least 90 days. ○ Visitor logs were kept at the office reception. Visitor badges were physically distinct from employee badges and no permissions were provisioned as visitor cards were intended for identification purposes only. ○ The offices implemented a clean desk policy. ○ A server room was hosted in the Lausanne office. The temperature in the office was monitored and air conditioning was available in the server room. CCTV was also enabled at the access points to the server room. ○ Uninterruptible power supply (UPS) units were available on the Lausanne site to power the server rooms in case of a power outage. ○ Where applicable, additional controls apply for access to IT rooms where IT media was stored.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-076 - Privacy Terms and Consent Notices Ensure that the following requirements are duly documented and agreed by customers in the Contractual Agreements: - Privacy terms - Consents - Intended use - Notices - 3rd party Sub-processors.	• Inspected evidence of a service agreement signed with a customer to determine whether processes were in place to communicate with customers about service requirements. • Inspected a random sample of onboarded customers to determine whether appropriate requirements were duly documented and agreed by customers in the Contractual Agreements.	No exceptions noted
ID-077 - Privileged Account Management (PAM) Nexthink defines policies and procedures to manage all privileged accounts by ensuring the principle of least privilege, mandatory Multi-Factor Authentication (MFA) and separation of privileges. Privileged accounts are reviewed on a periodic basis.	• Inspected evidence from Okta to determine whether MFA was enabled for all members of the organization, including administrator users. • Inspected evidence to determine whether reviews of the IT privileged accounts had been performed during the audit period.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-079 - Production System Monitoring and Paging Nexthink proactively monitors the Nexthink Experience service and supporting infrastructure on a 24/7 basis. Critical alerts are sent to an on-call engineer from the Cloud Operations team.	• Inspected a random sample of critical alerts raised in the monitoring tool to determine whether the alerts were sent to the Cloud Operations team.	Exceptions noted: EY could not obtain sufficient evidence to confirm that all the selected alerts were sent to the Cloud Operations team. EY gained the understanding that this is due to the cleanup of the used mailbox. **No further exceptions noted**
ID-080 - Protection of secret information Nexthink ensures that Nexthink Experience production keys and secrets are securely stored and protected.	• Inspected evidence of the components of the cloud environment to determine whether solutions were enabled for securely storing production keys and secrets.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-081 - Responsible Disclosure Process Nexthink runs a responsible disclosure program where customers and external security researchers are encouraged to responsibly disclose any vulnerability to Nexthink about its infrastructure or products and provided with clear guidelines and communication channels.	• Inspected evidence to determine whether channels were in place to facilitate that external parties can report identified vulnerabilities. • Inspected a random sample of reported vulnerabilities to determine whether vulnerabilities reported by external parties were investigated.	Exceptions noted: EY noted for 3 out of 5 samples not enough evidence could be provided to confirm that an investigation was performed regarding the reported vulnerability. **No further exceptions noted**
ID-082 - Review of access rights User access permissions are reviewed as part of ongoing security monitoring as defined in the Access Control policy.	• Obtained evidence of the access infrastructure code for engineering roles to determine whether the new infrastructure was put in place in September 2021. Determined that the annual reviews were not yet due as of the time of the audit procedures. • Inspected evidence of the latest performed Active Directory user review to determine whether the review was performed appropriately.	Exceptions noted: Based on inspection of the content of the review performed in April 2022 noted that only user information is reviewed but access permissions were excluded from the scope of the Active Directory review. **No further exceptions noted**

Control Activity	Tests Performed	Test Results
ID-083 - Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.	• Inspected the Risk Management Procedure to determine whether a methodology was in place for identifying, assessing, managing and monitoring risks. • Inspected evidence to determine whether a GRC tool was in place to register and monitor the state of identified risks. • Inspected a random sample to determine whether risk reviews were performed on an annual basis.	Exceptions noted: EY noted for 6 out of 25 samples the risk reviews were not completed in a timely manner. **No further exceptions noted**
ID-084 - Role-based access control (RBAC) Nexthink provisions access to systems following a role-based access control (RBAC) methodology, where employee access is based on their role.	• For engineering access, inspected the configuration of the RBAC4Engineering repository to determine whether: ○ Code owners (approvers) were defined for roles ○ Changes without a pull request and deletion were not permitted in the repository ○ Pull requests must have a minimum number of approvals of code owners • From the inspection of the history of commits gained comfort that the configuration has been available since the beginning of the audit period. Moreover, any changes on the configuration would have been subject to a pull request. • Inspected a random sample of newly added users on Active Directory to determine whether the access set-up was appropriate.	Exceptions noted: EY noted for 1 out of 12 samples the new user received one additional permission that was not defined for the job position. Further, gained the understanding that the client identified the exception through internal detective controls and applied corrective actions. **No further exceptions noted**

Control Activity	Tests Performed	Test Results
ID-085 - Secure Design and Application Threat Modeling Development teams receive feedback from architecture analysis, to ensure that the product is compliant with the Application Security Baseline. - Threat Modeling guideline - Definition of Ready (DoR) - Security Design Review – DoR.	• Inspected evidence to determine whether guidelines and standards were defined and communicated to the development teams to support with compliance requirements for secure design and development. • Determined whether a requirement for secure design review was integrated in the development process. • Inspected a random sample of development tasks to determine whether Definition of Ready checklist were completed.	Exceptions noted: EY noted for 5 out of 25 samples the DoR checklists were not explicitly documented. **No further exceptions noted**
ID-086 - Secure File Sharing Exchange of sensitive information with customers is performed via secure file transfer which implements end-to-end encryption.	• Inspected evidence to determine whether encryption tools were enabled in the support desk tool to facilitate the secure transfer of information shared with customers.	No exceptions noted
ID-088 - Security & Privacy Documentation Management The Policy Management Process describes how the documentation relevant to the Information Security Management System (ISMS) is governed, managed, maintained, and disseminated. Documents are re-viewed on a yearly basis following the Documentation Procedure.	• Inspected the content of the ISMS Documentation Procedure to determine whether review and update requirements were defined for maintaining the documentation of policies and procedures related to the Information Security Management Systems to ensure suitability, adequacy and effectiveness. • Inspected a random sample of policies maintained by the organization to determine whether procedures and policies were documented in line with the requirements and were reviewed.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-089 - Security & Privacy Governance Program Nexthink's security and privacy program maintains documentation of high-level policies and lower level controls and procedures. The policies and procedures cover the design, development, implementation, operation, maintenance and monitoring of in-scope systems. Controls are developed and maintained following objectives, risk assessments, compliance, or customer requirements.	• Inspected evidence to determine whether a Security Governance Policy and a Privacy Program was in place with description of objectives, roles, responsibilities, and resources in place to achieve security and privacy objectives. • Inspected a random sample of security and privacy documents to determine whether they had been reviewed. • Inspected evidence to determine whether a 3-year audit plan was in place. • Furthermore, determined that internal and external audits were organized to support with the evaluation of the controls.	No exceptions noted
ID-090 - Security & Privacy Roles and Responsibilities Security roles and responsibilities are defined and communicated for all personnel. Security governance policy and Acceptable usage policy defines roles and responsibilities.	• Inspected the content of the Security Governance Policy and the Acceptable Usage Policy to determine whether security-related roles and responsibilities were defined and documented.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-091 - Security Awareness & Trainings Nexthink provides mandatory security and privacy awareness training to its employees which must be completed within first three months of joining Nexthink (initial training) and annually (continuous training). Nexthink provides technical trainings to engineers aligned to the sensitivity of the data and systems they are required to perform their job duties which must be completed annually.	• Inspected a random sample of new joiners to determine whether mandatory new joiner trainings had been timely completed.	Exceptions noted: EY noted for 2 out of 12 samples the mandatory trainings were not completed in a timely manner. **No further exceptions noted**
ID-092 - Security Incident Response Process The Incident Management policy and plan are implemented, maintained, and disseminated; they include: - Roles and responsibilities. - Classification - Communication Channels - Tooling - Reporting - Playbooks for common incident types - Test plans - Lessons learned postmortem.	• Inspected a random sample of alerts from Hive to determine whether incidents assessments were performed, and identification and containment / eradication tasks were completed.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-093 - Security Objectives, Architecture and Design Nexthink documents its security architecture, including system and infrastructure security diagrams. Security principles and high-level security best practices are embedded in Nexthink's security strategy, and used as a reference when designing, implementing, and operating our Information Security Management System. Ensure during creation and review of Cloud Security policy and Engineering policy that these principles are present and updated if required.	• Inspected evidence to determine whether the security architecture for the cloud and infrastructure components had been documented and reviewed. • Inspected the content of the Cloud Security Policy and the Engineering Security Policy to determine whether dedicated sections describe the principles that must be complied with and whether these policies were reviewed.	No exceptions noted
ID-094 - Security posture monitoring Nexthink continuously scans resources deployed in AWS accounts to ensure they are aligned with the AWS Services Secure Configuration Standard and deviations are reported and acted upon.	• Inspected a random sample of alerts to determine whether deviations from the AWS services secure configuration standard were acted upon.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-095 - Segregation of cloud environment Production, pre-production, testing, and development environments are segmented by dedicated AWS accounts. Deliverables must follow the change management process to change from one environment to another. Production environment is also designed to separate customer data in a hybrid single and multi-tenant architecture.	• Inspected the Cloud Security Standard documentation to determine whether a structure was defined to implement the segregation between production and pre-production environments. • Inspected evidence from AWS to determine whether the structure and organization of AWS accounts corresponds to what was defined in the internal documents. • Inspected a random sample of deployed releases to determine whether releases were deployed in pre-production environments before they were implemented in production.	No exceptions noted
ID-096 - Service and Recovery Accounts Nexthink securely manages credentials of service accounts, which includes IP allow-listing and temporary credentials using the AWS Security Token Service. Recovery accounts are maintained to ensure emergency access to selected critical services.	• Inspected evidence of the configuration of IAM roles (service accounts) in AWS to determine whether access restrictions were defined in the form of temporary credentials and IP allow-listings. • Inspected a random sample of IAM roles (service accounts) to determine whether the accounts were appropriately configured.	No exceptions noted
ID-097 - Shared Responsibility Model Nexthink has created a responsibility map based on the Software-as-a-Service model where the different areas of responsibility can be clearly identified.	• Inspected evidence of a shared responsibility model to determine whether processes were in place to clearly identify customers responsibilities. • Inspected a random sample of onboarded customers to determine whether responsibilities were clearly identified.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-098 - Single Sign-On & Multi-Factor Authentication Nexthink implements single sign-on through Okta and Multi-Factor Authentication (MFA) to enable centralized management of identities and strong authentication. When technically possible, critical business applications must use an authentication system providing SSO capabilities based on Nexthink's centralized user directory.	• Inspected evidence from the authentication tool to determine whether MFA was enabled for all user types. Furthermore, determined that Single Sign On was enabled for internal applications. • Inspected a random sample of critical applications to determine whether risks and business justifications were recorded for critical applications that do not use SSO.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-100 - Software Development Process Nexthink maintains a secure software development process, coding standards, and release strategy to ensure security is built-in to the products and applications. Cloud infrastructure changes and software code de-ploys follow a defined change request process with automated and/or manual reviews and approvals. Provisioning of any production system requires a change request that is reviewed and approved by engineering.	• Inspected a random sample of development tasks that were part of the new product versions released to determine whether the changes adhered to the Software Development Process.	Exceptions noted: EY noted: • For 5 out of 25 samples the DoR checklists were not explicitly documented. • For 3 out of 25 samples no test evidence was available for the development task. EY noted that tests were performed on the release versions where the stories where deployed. • For 7 out of 25 samples the result of software component analysis was not available. • For 2 out of 25 samples EY noted that DoD checklists were not explicitly documented. **No further exceptions noted**

Control Activity	Tests Performed	Test Results
ID-101 - Source Code Management Nexthink stores its source code in an internal version control system, ensuring source code supporting Nexthink Experience is securely stored, accessed, and audited.	• Inspected a random sample of repositories that contain productive code to determine whether an audit log was available and that code reviews were enforced as part of the repository configuration. • Inspected the automated workflow for granting access to the repositories.	No exceptions noted
ID-102 - Special interest groups Nexthink maintains relationship with special interest group for technological watch, incident response and regulatory requirements.	• Inspected evidence to determine whether employees of Nexthink had active subscriptions during the audit period to professional groups that cover subjects related to information security.	No exceptions noted
ID-106 - Threat Intelligence Monitoring Stay up to date with the latest threat intel news related to threats and security risks that might impact Nexthink. The Security Team subscribes to news, feeds, forums, and special interest groups to receive updates on threat-intelligence and updates on applicable regulations and compliance.	• Inspected evidence to determine whether Nexthink follows-up on the development and qualification of employees from the security function, including the completion of required qualifications. • Inspected evidence to determine whether mechanisms were in place to share current knowledge about security threats and risks. • Inspected a random sample of alerts to determine whether the issues were resolved.	No exceptions noted
ID-109 - Tools Used for Auditing and Security Assessments Upon budgetary planning, the Security team reviews the existing and the needs for additional tooling or services.	• Inspected evidence of internal documentation to determine whether a review was performed during the audit period to evaluate determine the tools, resources and services needed to support the defined security strategy.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-110 - Understanding the Policies and Controls/Procedures Different documents used as part of the information Security Management System are clearly defined and documented. Ensure that all documents used in the ISMS follow the documentation procedure.	• Inspected the content of the ISMS Documentation Procedure to determine whether review and update requirements were defined for maintaining the documentation of policies and procedures related to the Information Security Management Systems in order to ensure suitability, adequacy and effectiveness. • Inspected a random sample of procedures and policies to procedures and policies were documented in line with the requirements and were reviewed.	No exceptions noted
ID-112 - User Endpoint Security Controls and Configuration Nexthink maintains security configurations across endpoints using Mobile Device Management systems. Nexthink implements restrictions to ensure that access to production environments is restricted to company managed devices. Nexthink denies by policy the usage of devices that are not managed or owned by the company (BYOD).	• Inspected evidence of the device management solution to determine whether company-owned and company-managed devices were registered and monitored. • Inspected evidence of the device management solutions used to provisioned endpoint devices with the applicable endpoint security policies to determine whether security policies were enabled for firewall protection, encryption, malware protection and removable media control. • Inspected evidence of the results of the review of privileged access accounts to determine whether a review of privileged accounts was performed during the period.	No exceptions noted

Control Activity	Tests Performed	Test Results
ID-113 - Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.	• Inspected the content of the Third-Party Assessment and Monitoring Procedures to determine whether processes were defined for: ○ Assessing and approving new vendors, ○ Monitoring existing vendors based on the risks identified during the initial assessment process. • Inspected a random sample of newly onboarded vendors to determine whether security assessments were performed before onboarding new vendors.	Exceptions noted: EY noted for 6 out of 25 samples the risk reviews were not completed in a timely manner. It was noted that one of the risks int the sample was related to a third-party review. **No further exceptions noted**
ID-115 - VPN Remote Access Nexthink provides its employees with a secure VPN to access the corporate network remotely through an encrypted tunnel, using client-side TLS certificates and enforced multi-factor authentication based on MFA.	• Determined that MFA was enforced to access Zscaler, the VPN solution. From inspection of the policies from the tool determined that Zscaler supports hardware-based inspection with TLS. Furthermore, from inspection of the Zscaler configuration, determined that access policies were defined for applications hosted in the corporate network.	No exceptions noted

ID-116 - Vulnerability and Patch Management Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure and across all systems managed by the IT team including servers and endpoints. Nexthink remediates security vulnerabilities based on their criticality and impact with a defined SLA.	• Inspected evidence from the Vulnerability Management Policy to determine whether a process was in place for identifying, monitoring and remediating system vulnerabilities. • Inspected evidence to determine whether a penetration test had been performed within the last year. • Inspected for a random sample of vulnerabilities to determine whether the vulnerabilities were remediated in a timely manner.	Exceptions noted: EY noted for 3 out of 21 samples of vulnerability reports, EY could not obtain sufficient evidence to confirm that the identified vulnerabilities were remediated based on the defined SLA requirements. EY gained the understanding that due to the limitations in the retention settings of the vulnerability scan history, the detailed results of the scan report were no longer available for inspection. For 1 out of 21 samples of vulnerability reports, EY noted that a selected vulnerability from the report was not resolved within the timeframe defined in the SLA. **No further exceptions noted**

Control Activity	Tests Performed	Test Results
ID-117 - Web Application Firewall Nexthink implements web application firewall technology to protects web resources from malicious attacks.	• Inspected evidence from Cloudflare to determine whether rules were configured to enable the protection of web resources from malicious attacks. • Inspected evidence for a random sample of changes to the web application firewall configuration to determine whether the changes were approved by IT.	No exceptions noted

5. Section V: Other Information

The following includes Nexthink's responses to **Results of Tests** as included in Section IV of this report.

Control Activity	Tests Results	Management Response
ID-002 - Access Establishment Modification and Termination Nexthink's HR Operations and IT teams deprovision user access upon employees leaving the company. Nexthink new-hires on-boarding is coordinated between HR and IT to ensure appropriate access provisioning and system configurations are in place for each new hire. The HRIS system (BambooHR) sends automated notifications to the IT ServiceDesk prior to employee onboarding. Nexthink follows a least privilege model based on RBAC applied for onboarding as well as role and access changes.	Exceptions noted: EY noted for 1 out of 12 samples of new access establishment, the new user received one additional permission that was not defined in the list of roles per job function. **No further exceptions noted**	Nexthink follows a least privilege model based on RBAC applied for onboarding as well as role and access changes. This is a preventive control. We have now implemented detective and corrective action for this control at the same frequency. This means two level checks are performed to verify that correct roles are assigned to the new employees at the time of onboarding. Additionally, we are also performing a quarterly check to review role assignment.

Control Activity	Tests Results	Management Response
ID-012 - Background Check Reviews Nexthink employees undergo systematic background screening prior to employment. The checks performed are aligned to the risk associated to the job position. Background checks are performed by the third-party HireRight.	Exceptions noted: EY noted for 3 out of 12 samples not enough evidence could be provided to determine whether a background check was performed. Furthermore, EY noted for 1 out of 12 samples the background check verification was not requested. **No further exceptions noted**	Nexthink uses HireRight application for managing background screening. The screening reports are scheduled to be permanently deleted from HireRight storage 6 months after completing the Screening Report. This is in accordance with GDPR as background screening reports contain PII. Hence, we could not provide evidence for 3 of the sampled employees. This is a scope limitation. HireRight sends a monthly 'Deletion Report' to confirm that the screening reports and related documents are permanently deleted. For providing evidence in future audits, we will add employee ID field in this report. This will show that background screening was performed but the screening report was deleted post 6 months, in compliance with GDPR. In the monitoring period, 186 employees were hired. For one of the sample, due to human error, background verification was not requested on the tool, which has been completed now. To avoid this in future, we have enabled the functionality in our application tracking system to make Background Check a mandatory step before moving a candidate to the Hired stage.

Control Activity	Tests Results	Management Response
ID-016 - Business Continuity and Disaster Recovery Test Plan Test exercises are performed according to policy.	Exceptions noted: EY noted for 3 out of 5 samples not enough evidence could be provided to confirm that test objectives were defined and that end-to-end tests were performed to validate the full scope of recovery activities. **No further exceptions noted**	We are modifying the BCDR Plan to include objectives, test procedures and recovery activities to be performed systematically during testing for every scenario. The BCDR plan will be communicated with relevant stakeholders to ensure BCDR plan is consistently implemented. We are also planning to engage with external subject matter experts to provide guidance for improving our crisis management and BCDR strategy.

Control Activity	Tests Results	Management Response
ID-019 - Change Management Nexthink has defined a change management process defining the different type, approval workflow and review. System management tools are provisioned following the same requirements and configurations as any production system. - All changes must go through pull requests with code reviews. - Deployment happens in the same way as for the product components themselves, through build pipe-lines. - Cloud system management tools are developed according to the SDLC (including Definition of Ready and Definition of Done).	Exceptions noted: EY noted for 5 out of 5 samples the changes did not follow the defined change process. In particular 2 changes were not formally tested, in addition, no comprehensive evidence was available to determine whether 4 changes were approved by appropriate persons. **No further exceptions noted**	Two of the sampled Maintenance Releases (MRs) - 2022.2.3, 2022.2.5, were related to a bug. The Cloud Platform team fixed the issue, but outcome of testing was not formally recorded in the associated Jira ticket. We are updating our change management process to record the outcome of tests in the associated tickets. For the release 2022.2.5, due to a miscommunication, formal approval from Quality Engineering was missing in the Pull Request (PR). We are updating our change management process to review permissions, update process document to mention who should approve, add the responsible person to the mailing list, and communicate the updated process to relevant stakeholders. For the releases 2022.2.5, 2022.5.1, 2022.1.2, 2022.4.1, platform release acceptance was provided by the Cloud Platform Engineering Manager as the other roles were undergoing organizational change. We are updating the documentation process of release acceptance by the platform team to explicitly mention the approvers. For the release 2022.1.2, approval from Quality Engineering was missing. To prevent this in future, we are improving our change management process to refactor the code, create a different release lifecycle and process for internal changes (these changes do not impact customers). The associated PR will explicitly mention internal/external change in the scope of the release.

Control Activity	Tests Results	Management Response
ID-036 - Emergency changes An emergency change process is in place. Details of any emergency change are retroactively documented and approved. Emergency changes are covered via: - The Internal bugs process for the SDLC and Cloud Platform - The high impact changes for CloudOps. - The emergency changes for IT Corporate.	Exceptions noted: EY noted for 3 out of 8 samples of cloud platform emergency changes the evidence of test results were not documented. EY that for 5 out of 5 samples the approval from the Cloud Operations Manager was not available. EY noted the process of approval of infrastructure maintenance releases was not in place during the report period. **No further exceptions noted**	We are updating our change management process for managing changes which do not impact customers (i.e., internal changes such integrations with our third-party tools or related to pipelines which do not involve code going into production). This includes improvement measures such as refactoring of code in order to split the code which is not production code, reviewing existing permissions, automating tests for production code and integrating automated quality gates. As an immediate remediation, we have enforced the current process by communicating with teams and reviewing permissions to guarantee that changes have gone through the process and obtained necessary approval.
ID-045 - Free and Open-Source Software (FOSS) Security Product dependencies (open or closed source) are scanned with a Software Component Analysis (SCA) tool looking for potential security vulnerabilities and licensing issues.	Exceptions noted: EY noted for 7 out of 25 samples the result of the software component analysis scan was not available, therefore, the test could not be performed for the selected samples. **No further exceptions noted**	SCA evidence was not available due to a tool limitation on the vendor's side (tool was unstable when integrated with XRay and Artifactory). This was a scope limitation which has now been remediated.

Control Activity	Tests Results	Management Response
ID-079 - Production System Monitoring and Paging Nexthink proactively monitors the Nexthink Experience service and supporting infrastructure on a 24/7 basis. Critical alerts are sent to an on-call engineer from the Cloud Operations team.	Exceptions noted: EY could not obtain sufficient evidence to confirm that all the selected alerts were sent to the Cloud Operations team. EY gained the understanding that this is due to the cleanup of the used mailbox. **No further exceptions noted**	PagerDuty has been integrated with NewRelic, hence alert evidence will be available for future audits.
ID-081 - Responsible Disclosure Process Nexthink runs a responsible disclosure program where customers and external security researchers are encouraged to responsibly disclose any vulnerability to Nexthink about its infrastructure or products and provided with clear guidelines and communication channels.	Exceptions noted: EY noted for 3 out of 5 samples not enough evidence could be provided to confirm that an investigation was performed regarding the reported vulnerability. **No further exceptions noted**	Analysis of the 3 sampled reports was not conclusive of their validity. One of them was a low-risk vulnerability. The second one did not concern Nexthink assets hence was out of scope. The third vulnerability did not show any risk. However, we did not maintain any proof / evidence to show the analysis of these sampled vulnerabilities. As an improvement to the responsible disclosure process, we have created a shared mailbox for responsible disclosure, and added an automatic message to acknowledge each email. We now document the analysis of the reported vulnerabilities (i.e., if the vulnerability is valid and requires remediation or not) in an associated ServiceNow ticket (if relevant) or directly in the responsible disclosure mailbox.

Control Activity	Tests Results	Management Response
ID-082 - Review of access rights User access permissions are reviewed as part of ongoing security monitoring as defined in the Access Control policy.	Exceptions noted: Based on inspection of the content of the review performed in April 2022 noted that only user information is reviewed but access permissions were excluded from the scope of the Active Directory review. **No further exceptions noted**	Nexthink provisions access to systems following RBAC methodology, where employee access is based on their role. Hence, user access permissions review means that their roles are reviewed. IT reviews and updates roles when informed by HR about a person's role change. This includes offboarding cases also. Applications with Single Sign On (SSO) are automatically deprovisioned by the automation system. IT also has a check for every onboarding performed by a different team member to verify that the correct roles have been assigned on user creation and provisioning. Role review is performed when HR triggers the role change process for an employee. Manual access review of applications with SSO is in progress and expected to be completed by Q4 2022. We are automating the access review process and currently conducting PoC of access review tools.

Control Activity	Tests Results	Management Response
ID-083 - Risk Management Process A process describes how to conduct, manage, govern, and maintain the information security risk management activity and its related documentation and outcomes.	Exceptions noted: EY noted for 6 out of 25 samples the risk reviews were not completed in a timely manner. **No further exceptions noted**	We moved from Eramba (our previously used GRC tool) to ServiceNow in 2022. We expected to review risks from 2022 onwards in the new tool. However, as Eramba used a different compliance framework than ServiceNow, the go-live was delayed due to mapping issues. Hence, the risks expired in Q1 2022 were reviewed late in ServiceNow. The ISMS Management Committee (CTO, CFO) acknowledged the delay in late review of 4 of these sampled risks. In the risk review process, sometimes, there are delays in getting response from the risk owners due to their limited availabilities (leaves, shifting of review meetings due to other business priorities, delay in response, etc.). This explains the delay for the other two sampled risks. Review for all the sampled risks for which deviation was noted have been completed. None of these risks had any significant impact on the Nexthink's security posture. We have updated our risk management process to initiate the risk review process before its expiration date. We maintain a monthly KPI to monitor risk exposure and check expired risks. If found, corresponding risk review tasks are created. In risk review is delayed for any business reason, its justification is recorded in ServiceNow.

Control Activity	Tests Results	Management Response
ID-084 - Role-based access control (RBAC) Nexthink provisions access to systems following a role-based access control (RBAC) methodology, where employee access is based on their role.	Exceptions noted: EY noted for 1 out of 12 samples the new user received one additional permission that was not defined for the job position. Further, gained the understanding that the client identified the exception through internal detective controls and applied corrective actions. **No further exceptions noted**	Nexthink follows a least privilege model based on RBAC. This model is applied for onboarding as well as role and access changes as a preventive ad-hoc control. We have now implemented detective and corrective action for this control at the same frequency. This means two level checks are performed to verify that correct roles are assigned to the new employees at the time of onboarding. Additionally, we are also performing a quarterly check for role verification.
ID-085 - Secure Design and Application Threat Modeling Development teams receive feedback from architecture analysis, to ensure that the product is compliant with the Application Security Baseline. - Threat Modeling guideline - Definition of Ready (DoR) - Security Design Review – DoR.	Exceptions noted EY noted for 5 out of 25 samples the DoR checklists were not explicitly documented. **No further exceptions noted**	DoR is not a mandatory requirement. When a story is created, users get a pop-up to go to Ready state showing a reminder of everything that needs to be completed from a quality point of view, to be allowed to go to this state. The developer checks the box stating that they comply with the full list. The button to close the pop-up works even if the checkbox is not checked. So, for these sampled stories, the developer did not select the checkbox. However, we are updating the Jira workflow to explicitly mention if the DoR checkbox was not clicked at the time of creation.

Control Activity	Tests Results	Management Response
ID-091 - Security Awareness & Trainings Nexthink provides mandatory security and privacy awareness training to its employees which must be completed within first three months of joining Nexthink (initial training) and annually (continuous training). Nexthink provides technical trainings to engineers aligned to the sensitivity of the data and systems they are required to perform their job duties which must be completed annually.	Exceptions noted EY noted for 2 out of 12 samples the mandatory trainings were not completed in a timely manner. **No further exceptions noted**	As per updated control definition, mandatory trainings must be completed within 90 days. The sampled employees for whom deviation was noted have completed their mandatory trainings. To ensure new joiners complete the mandatory trainings within 3 months of their joining, monthly reminders are sent through the Learning Management System (LMS) tool. We maintain a monthly KPI for Security & Privacy awareness & training program with target as: - at least 90% of employees must complete Security and GDPR training. - at least 95% of employees must complete Engineering Security training. Additionally, we maintain a quarterly KPI that at least 90% of employees must complete the annual refresher of Security and GDPR training. If metrics are not met, we send the awareness campaign, follow-up with managers and review the awareness campaign if there is no improvement.

Control Activity	Tests Results	Management Response
ID-100 - Software Development Process Nexthink maintains a secure software development process, coding standards, and release strategy to ensure security is built-in to the products and applications. Cloud infrastructure changes and software code de-ploys follow a defined change request process with automated and/or manual reviews and approvals. Provisioning of any production system requires a change request that is reviewed and approved by engineering.	Exceptions noted: EY noted • For 5 out of 25 samples the DoR checklists were not explicitly documented. • For 3 out of 25 samples no test evidence was available for the development task. EY noted that tests were performed on the release versions where the stories where deployed. • For 7 out of 25 samples the result of software component analysis was not available. • For 2 out of 25 samples EY noted that DoD checklists were not explicitly documented. **No further exceptions noted**	DoR and DoD are not mandatory requirements. When a story is created, users get a pop-up to go to Ready state showing a reminder of everything that needs to be completed from a quality point of view, to be allowed to go to this state. The developer checks the box stating that they comply with the full list. The button to close the pop-up works even if the checkbox is not checked. So, for these sampled stories, the developer did not select the checkbox. However, we are improving the Jira workflow to explicitly mention if the DoR/ DoD checkbox was not clicked at the time of creation. For the sampled development stories for which deviation was noted, tests were performed on the release in which the stories were included. SCA evidence was not available due to a tool limitation on the vendor's side (tool was unstable when integrated with XRay and Artifactory). This was a scope limitation which has been now remediated.

Control Activity	Tests Results	Management Response
ID-113 - Vendor Management A vendor management process is in place to assess the security maturity and risk of new vendors being on-boarded and ensure the risk is tracked appropriately.	Exceptions noted EY noted for 6 out of 25 samples the risk reviews were not completed in a timely manner. It was noted that one of the risks in the sample was related to a third-party review. **No further exceptions noted**	We moved from Eramba, our previous GRC tool, to ServiceNow in 2022. We expected to review risks from 2022 onwards in the new tool. However, as Eramba used a different framework than ServiceNow, the go-live was delayed due to mapping issues. Hence, the risks expired in Q1 2022 were reviewed late in ServiceNow. The ISMS Management Committee (CTO, CFO) acknowledged the delay in late review of 4 of these sampled risks. In the risk review process, sometimes, there are delays in getting response from the risk owners due to their limited availabilities (leaves, shifting of review meetings due to other business priorities, delay in response from vendors for documentation, etc.). This explains the delay for the other two sampled risks. Review for all the sampled risks for which deviation was noted have been completed. None of these risks had any significant impact on the Nexthink's security posture. We have updated our risk management process to initiate the risk review process before its expiration date. We maintain a monthly KPI to monitor risk exposure and check expired risks. If found, corresponding risk review tasks are created. If risk review is delayed for any business reason, its justification is recorded in ServiceNow.

Control Activity	Tests Results	Management Response
ID-116 - Vulnerability and Patch Management Nexthink identifies, assesses, tracks, and actively remediates vulnerabilities in Nexthink Experience, its underlying infrastructure and across all systems managed by the IT team including servers and endpoints. Nexthink remediates security vulnerabilities based on their criticality and impact with a defined SLA.	Exceptions noted EY noted for 3 out of 21 samples of vulnerability reports, EY could not obtain sufficient evidence to confirm that the identified vulnerabilities were remediated based on the defined SLA requirements. EY gained the understanding that due to the limitations in the retention settings of the vulnerability scan history, the detailed results of the scan report were no longer available for inspection. For 1 out of 21 samples of vulnerability reports, EY noted that a selected vulnerability from the report was not resolved within the timeframe defined in the SLA. **No further exceptions noted**	Data Retention Policy in our vulnerability management tool (Tenable.SC) is 180 days. During the audit, evidence for some of the samples were lost as 180 days had expired. Hence for some of them, details of the vulnerabilities could not be provided. Nevertheless, we provided the evidence for analysis of vulnerabilities that was communicated to the stakeholders (via) email as evidence. This is a scope limitation. We have increased the data retention time of the vulnerability management tool to preserve the evidence for longer periods of time for future audits. The vulnerability for which deviation is noted is AMQP Cleartext Authentication (Medium severity). This vulnerability is downgraded to Low as it is related to the tools - Xray and Artifactory and to not our code. We will redeploy Xray and fix the issue by December 2022.