

nexign

Nexign JSC

Services “Delivery”, “Technical Support”, “Managed Services”

Service and Organization Controls (SOC) 3[®] Report
for the period from December 1, 2023 to November 30, 2024

ДРТ

ДЕЛОВЫЕ РЕШЕНИЯ И ТЕХНОЛОГИИ

BUSINESS SOLUTIONS AND TECHNOLOGIES

Table of contents

Section I: Independent Service Auditor's Report	3
Section II: Management's Assertion	6
Section III: System Description as Provided by Management	8
Section IV: Principal Service Commitments and System Requirements	16

Section I: Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

Nexign JSC

4, Uralskaya st., St. Petersburg, Russian Federation

Scope

We have examined the accompanying assertion of Nexign JSC related to services "Delivery", "Technical Support", "Managed Services" of Nexign JSC and Nexign Solutions LLC ("Nexign", the "Service Organization") throughout the period from December 1, 2023 to November 30, 2024 (the "assertion") that the controls stated in the description were effective throughout the period from December 1, 2023 to November 30, 2024, to provide reasonable assurance that Nexign's services commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in *TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Nexign uses JSC Atomdata-Center (Xelent), LLC Svyaz VSD (Linxdatacenter) and JSC Severen-telecom ("subservice organizations") for its hardware hosting in the data centers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nexign, to achieve Nexign's services commitments and system requirements based on the applicable trust services criteria. The description presents Nexign's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nexign's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

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

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

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

Opinion

In our opinion, management’s assertion that the controls within Nexign’s system related to services “Delivery”, “Technical Support”, “Managed Services” were effective throughout the period December 1, 2023 to November 30, 2024, to provide reasonable assurance that Nexign’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

AO Business Solutions and Technologies

December 27, 2024

Moscow, Russia

Section II: Management's Assertion

Management's Assertion

To: AO BST

5 Lesnaya St., Moscow, 125047, Russia

We are responsible for designing, implementing, operating, and maintaining effective controls within Nexign JSC and Nexign Solutions LLC ("Nexign" – Service Organization) Service Organization's system related to services "Delivery", "Technical Support", "Managed Services" of Nexign, throughout the period December 1, 2023 to November 30, 2024, to provide reasonable assurance that Nexign's service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system (the "Description") is presented in Section III and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 1, 2023 to November 30, 2024 to provide reasonable assurance that Nexign's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Nexign's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section IV.

Nexign uses JSC Atomdata-Center ("Xelent"), LLC Svyaz VSD ("Linxdatacenter"), JSC Severen-telecom for its hardware hosting in the data centers. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nexign, to achieve Nexign's services commitments and system requirements based on the applicable trust services criteria. The description presents Nexign's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Nexign's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

This assertion the Description related to services "Delivery", "Technical Support", "Managed Services" indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nexign to achieve the Nexign's service commitments and system requirements related to Nexign system based on the applicable trust services criteria. The accompanying Description presents the complementary user entity controls assumed in the design of Nexign's controls.

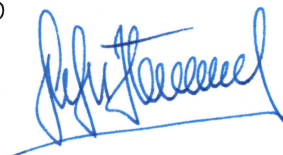
There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements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

We assert that the controls within the system were effective throughout the period December 1, 2023 to November 30, 2024 to provide reasonable assurance that Nexign's service commitments and system requirements were achieved based on the applicable trust services criteria.

Mikhail Matyushin, CEO

Nexign JSC

December 27, 2024



Section III: System Description as Provided by Management

Overview of Operations

Company Background

Nexign, JSC is a developer of high-tech enterprise solutions for various industries. Nexign products support our customers' transformation by helping to harmonize business processes, create an employee digital ecosystem, and increase the efficiency of IT departments.

From converged BSS systems to sophisticated secondary software optimization solutions, Nexign's broad product line provides a comprehensive approach to reengineering any business processes. Customer interests always come first for Nexign.

Our deep technical expertise enables us to successfully and transparently execute projects of any size and complexity while maintaining the continuity of all management and technology processes.

Nexign helps businesses transform at any level and always keep pace with the market.

Nexign offers integrated solutions for the execution and operation of BSS systems, associated software and equipment. The primary objective of the company is to provide telecom operators and clients from other industries with a full range of IT services based on the one-stop concept.

Business Description

Nexign provides the following services for clients:

Delivery – within the scope of this service Nexign implements solutions for its customers. Nexign uses various IT systems such as Jira, Confluence, Allure and messengers to ensure clear and transparent collaboration with the customer's team.

The purpose of the Delivery service is to implement the project as per contract agreements and aligned with customer expectations taking into account requirements on supplied solution and service quality.

Implementation is supervised by the Project Management Office (PMO), its responsibilities are to provide and monitor compliance with project management processes, policies and methods.

Delivery service is provided in several stages: Inception, Elaboration, Construction, Transition, Production.

At the Inception stage the business objectives, goals, and scope of the project are defined and the project's feasibility is established during requirement gathering activities that produce the high-level business models. Potential risks are identified and mitigation strategies for each risk are developed. The Project Management Plan is used to define the overall work to be performed on the project. An Iteration Work plan is developed to define the details of the work to be performed in the first iteration of the Elaboration phase.

During Elaboration phase the detailed requirements for implementation are developed, the project team's understanding of the business requirements is verified to reduce development risk.

During the Construction phase, validation of all components fit together, and preparation of the system for the acceptance test and deployment is performed.

During the Transition phase, the system is tested systematically to be available for end users. The system implementation is accepted by the customer organization, the organization is made ready for the new system, and the system is put into production and, if the new system replaces an old one, a smooth cutover to the new application is provided.

During the Production phase, the newly implemented system is monitored to address system issues. This includes monitoring the system and acting appropriately to maintain continued operation, measuring system performance, operating and maintaining supporting systems, and responding to help requests, error reports and feature requests by users.

Technical Support (TS) – Customers receive ongoing technical assistance and on-demand advisory support for solution operation from Nexign's expert team. Nexign offers a variety of programs according to the contracts with customers, including 24/7/365 support across multiple time zones.

Nexign provides consultations on the software in the form of responses to customer's requests posted in the protected section of the web server of Nexign Atlassian Jira.

In case when system maintenance is requested Nexign delivers patches and/or new versions of supported software by placing the distribution packages or update packages in the information system according to the signed agreement with the client.

Managed Services (MS) – Nexign Managed Operations Services ensure end-to-end application management, keeping the customer's operations running continuously.

Information with description of Nexign's services is available to customers on the Nexign website. Additional System description details are available for customers and potential customers through third-party audit and attestation reports are available upon request.

Scope of Managed Services service includes following groups of processes:

Inform & Restore process group

Event & Monitoring – monitors systems to ensure that they are working correctly, providing IT services according to the agreements, detecting issues as early as possible and initiating response activities.

Incident management – restores normal service operation as quickly as possible and minimize the adverse impact on business operations, thus ensuring that the agreed levels of service quality are maintained.

Problem management – seeks to minimize the adverse impact of incidents and problems on the business that are caused by underlying errors within the IT Infrastructure and to proactively prevent recurrence of incidents related to these errors. In order to achieve this, problem management seeks to get to the root cause of incidents, document and communicate known errors and initiate actions to improve or correct the situation.

Change & Deliver process group

Request fulfilment - fulfilment processes are to maintain user and customer satisfaction through efficient and professional handling of all service requests, to provide a channel for users to request and receive standard services.

Service requests are classified into three types for better process management:

- Access request – request for creation or change of system user accounts.
- Standard request – request for configuration of single product, request for actions with usage of system functionality or request for information/system data.
- Complex request – request for complicated configuration of several products.

IT operation control – execution of the ongoing activities and procedures required to manage and maintain the IT infrastructure so as to deliver and support IT services at the agreed levels.

Release and Deployment management – release and deployment management process that plans, schedules and controls the building, testing and deployment of releases, and delivers new functionality required by the business while protecting the integrity of the existing services.

Operational Change Management – provides guarantee of control of all application changes, prevent unapproved changes on the system and thereby improve system stability and availability.

Prevent process group

Capacity management – is the practice of right-sizing IT resources to meet current and future needs.

Availability management – aims to define, analyze, plan, measure and improve all aspects of the availability of IT services. It is responsible for ensuring that all IT infrastructure, processes, tools, roles etc. are appropriate for the agreed availability targets.

Continuity Management – aims to manage risks that could seriously impact IT services. This process ensures that Nexign can always provide minimum agreed Service Levels, by reducing the risk from disaster events to an acceptable level and planning for the recovery of services.

Security Management – control access to information.

Agree process group

Service Level Management – negotiating Service Level Agreements and ensuring that these are met. Includes customer satisfaction surveys, monthly meetings to discuss the quality of service, critical problems and other important questions for guarantee all processes are appropriate for the agreed service level targets.

Requirement engineering – is a customization process that lays ground for on-demand application development and accompanying business process creation, configuration or adjustment. Effort estimation for requirement engineering service is predefined in the agreed quota and can be used when necessary and confirmed by both parties based on the contract conditions.

Improve process group

Continual Service Improvement – continually improve the effectiveness and efficiency of Managed Services processes and BSS services, delivered by Nexign software.

Knowledge management – process of creating, sharing, using and managing the knowledge and information of technical support groups and levels.

Applicability of the Description

This Description has been prepared to provide information on Nexign System: Delivery, Technical Support and Managed services process internal controls that may be relevant to the requirements of its customers to meet security and availability criteria.

As such, the detail herein is intended to meet the common requirements of a broad range of users and may not, therefore, include every aspect of the System that each customer may consider important. Furthermore, detail is limited to the controls in operation over the System described below. The authorized users of the Systems supporting the internal controls are limited to the applicable Nexign personnel.

Scope Boundary

The following Nexign services are in scope for this report:

- Delivery services – full process;
- Technical support – full process;
- Managed services – full process.

Nexign Datacenters

Nexign, JSC uses JSC Atomdata-Center (Xelent), LLC Svyaz VSD (Linxdatacenter) and JSC Severen-Telecom (RTK-DC) for its hardware hosting in the data centers. Datacenter employees are responsible for the physical security of the data centers, data protection, and physical hardware asset management and network services. Besides that Nexign cells in the data centers are managed, monitored, and operated by Nexign IT staff delivering online services with 24x7x365 continuity. Nexign also maintains and manages network and platform security.

People

Nexign personnel is organized into service teams that develop and maintain the application and the support teams that provide supporting services for System operations. Teams external to Nexign also support system operations. Each service and support team has defined responsibilities and accountabilities to manage security, availability, processing integrity and confidentiality of the application. The teams include the following working groups:

- Nexign IT and TS/MS teams include development, testing, and project management teams tasked with developing and maintaining the Nexign applications.
- Technical risk management council that consists of representatives from Delivery, TS\MS and IT personnel provides a single resource to assist Nexign teams in analyzing continuity and disaster recovery requirements, documenting procedures, and conducting testing of established procedures.
- Data Center Software Services (DSS) supports Nexign by managing the requesting, scheduling, and restoration of backups.

- Nexign Security working group responsible for Security issues within the Nexign environment. The working group is comprised of personnel from multiple groups throughout the business.
- Governance, Risk, and Compliance (GRC) identifies, documents, and advises teams in implementing controls to maintain Nexign solution's security, availability, processing integrity and confidentiality commitments to its customers.
- Information Technology (IT) provides the access control and authentication mechanism for the corporate network, maintain AD services, authentication rules and user access, so as identifies and communicates technical vulnerabilities associated with Nexign assets.
- Nexign Managed Operations Services ensure end-to-end application management, keeping the customer's operations running continuously. The benefits of adopting our Managed Operations Services include faster incident resolution and request fulfilment, minimized impact of staff error, reduced impact of incidents, increased process efficiency, downtime risk mitigation and faster Time-to-Market (TTM) for new products.

Organizational structure, reporting lines, authorities are described within HR procedures and internal portal (Neon).

HR administration group's responsible employee revise organizational structure as part of HR Governance process and make changes as needed at least once a year.

Procedures

Nexign adheres to Information Security Management System. The purpose of the Information Security Management System is to ensure the confidentiality of Nexign information, including customer information, access to information, business continuity and risk of loss, by preventing information security incidents and their potential impact. This System defines accountability and responsibility for implementing security and evaluating efficacy of security controls. The ISMS applies to the following IT services:

- Email (E-MAIL)
- Network
- Workplace (Desktop)
- Remote access to customers' networks
- Customer File Transfer Management (Customer MFT)
- Clients FileShare
- Internet access
- Remote access to internal information resources (VPN access)
- Active Directory
- Accounting and processing of user requests (Service Desk)
- Backup (BackUp)
- Equipment rent
- System Center Configuration Management (SCCM)
- Virtual Workplace (VDI)
- Internal passes
- Support for automated solutions based on JIRA software (JIRA)
- Testing process management system (TestRail, Allure)
- Data Center infrastructure
- Enterprise wiki (Confluence)
- Installing Security Updates on NIX Servers
- Installing Security Updates on WIN Servers
- Remote Access for Contractors

- Ensuring continuous integration (Continuous Integration by TeamCity, Jenkins)
- Version Control System and Code Review (Bitbucket / Stash, Gitlab)
- Privileged User Control (PUM)
- Certification Center (PKI)
- Unified storage of artifacts (Artifactory)
- IT service availability monitoring (Zabbix)
- Recruitment process automation (JIRA-HR)
- Corporate portal "neon"
- Electronic Document Management (ECM)
- Check-In
- Outsource management
- Identity Management (IDM)

Data

Nexign customer content is maintained in Nexign internal systems. Each service and support team is responsible for managing the security and availability of the data in Nexign systems. The table below details the data classifications for this report and the Nexign environment.

Category	Who can get an access	Storage and access requirements
Internal information (II), such as <ul style="list-style-type: none"> - algorithms, source codes, modules used, project documentation, operational documentation; - technical projects; - technical assignments; - technical and functional specifications; - software acceptance test protocols; - working materials for analyzing the work of the software being developed; - information about the principles and methods of security. 	<ul style="list-style-type: none"> • All employees of the Organization who need access to this information to perform their job duties; • Employees of the Organization's counterparties who need access to it in order to fulfill their obligations under the agreement with the Organization 	<ul style="list-style-type: none"> • Restriction of access to II (both at the physical level and at the logical level in the IR)
Critical commercial information (CCI), such as <ul style="list-style-type: none"> - financial terms of contracts; - financial and economic information; - the financial component of commercial proposals, which is sent to potential clients; - non-impersonal information about customer subscribers; - passwords from client systems and servers; - domain password of an NX employee from his user account; - passwords issued to counterparties to access the NX network. 	<ul style="list-style-type: none"> • Management of the Organization • A limited and controlled by the Security Department (SD) number of employees who are either the executors of documents with the CCI, or who need access to the CCI to perform their job duties or who have received permission to access it from the head of the structural unit. 	<ul style="list-style-type: none"> • Restriction of access to the CCI (both at the physical level and at the logical level in the IR) • Storage of CCI only in places permitted by SD in the corporate network of the Organization

Software

Nexign uses a joint information platform supporting collaborating process for providing effective Customer service:

- Jira – Events, Incidents, Problem, and Software requirements Specification «Atlassian JIRA» software product is used as a ticketing platform. Jira project and task management system allows users to work with several projects. Split them to stages, configure type of tasks, connect tasks with each other, assign responsible for activities, configure project roles, form reports etc.
- Confluence – project documents and Knowledge base, reports, process documentations, Service and system information papers& instructions. Confluence is a collaboration wiki tool used to help teams to collaborate and share knowledge efficiently. It allows organizing workspaces, file storage, discussion, and blogs. System consist of several key domains, which allows to find and organize content. Data in Confluence has a specific structure, which is divided to work spaces, access to which is restricted according to teams and responsibilities.

Development tools

- TestRail and Allure are web-based test case management tools. They are used by testers, developers and team leads to manage, track and organize software testing efforts. TestRail and Allure allow team members to enter test cases, organize test suites, execute test runs and track their results.
- Atlassian software product Bitbucket (Stash) and Gitlab are being used as platforms for version control, source code review and code review. Bitbucket (Stash) and Gitlab support quick versions splitting and merging, it includes instruments for visualization and navigation through nonlinear development history and for Pull Request creation. Every developer works with local copy of repository, after that changes are being copied to central repository located on server.
- TeamCity and Jenkins are build management and continuous integration software.

Complementary Subservice Organization Controls (CSOC)

The controls of Nexign Service Organization (hereinafter “Company”) that pertain to the defined processes “Delivery”, “Technical Support”, “Managed Services” and the controls over that processes were designed with the assumption that certain controls are in operation within the user entity. It is not feasible for the control objectives related to the processes “Delivery”, “Technical Support”, “Managed Services” to be achieved solely by Nexign. Therefore, User entity internal controls over financial reporting must be evaluated in conjunction with the Nexign’s controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization and Client controls expected to be implemented at the subservice organization and Client as described below.

Complementary Subservice Organization Controls (CSOC)		Related Criteria
1	Logical and physical access controls exist to provide reasonable assurance that unauthorized access is restricted by subservice organization.	CC6.1 CC6.2 CC6.4
2	Environmental controls are set up in the data center where application and database servers are located.	A1.2
3	The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.	CC6.6 CC6.8

Complimentary User Entity Control Considerations (CUEC)

Complimentary User Entity Control Considerations (CUEC)	Related Criteria
1 The Production environment is closed for changes for Nexign employees after project completion.	
2 A formal change control process exists to provide reasonable assurance that the promotion of changes to the production environment is done in a controlled manner consistent with management’s intentions. 3 Responsible user organizations’ employees are responsible for testing of improvements made in accordance with the user organizations’ request. Responsible employee of user organizations monitors activity of Nexign users, who got approved access to user organizations’ production or test environments.	CC8.1
4 Only authorized employees of the user organization have access to create service requests for Nexign services.	
5 Only authorized employees of the user organization have access to approve and accept service request processed by Nexign.	CC6.1 CC6.2 CC6.3
6 Only authorized employees of the user organization may block the accounts of Nexign employees in user organization systems based on requests from Nexign.	
7 On the Client’s side, the Internet Security Protocol (IPsec protocols) is configured.	CC6.7

Section IV: Principal Service Commitments and System Requirements

Service Commitments

Nexign makes service commitments to its customers and has established system requirements as part of services “Delivery”, “Technical Support”, “Managed Services”. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. Nexign 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 Nexign’s services commitments and system requirements are achieved. Service commitments to customers are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- Security: Nexign has made commitments related to securing customer data from both unauthorized remote and physical access. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.
- Availability: Nexign has made commitments related to effort to maintain availability of the service and user data to users to make sure that users’ data is accessible to users without significant interruptions.

System Requirements

Nexign designs its processes and procedures to meet its objectives for its services “Delivery”, “Technical Support”, “Managed Services”. Those objectives are based on the service commitments that Nexign makes to user entities, the laws and regulations that govern the provision of the Nexign services and the financial, operational and compliance requirements that Nexign has established for the services.

Nexign established the standardized processes and system requirements, which include, but are not limited to, the following:

- Access Security: Nexign maintains data access and logical security policies, designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data.
- Access to systems is restricted based on the principle of least privilege.
- Network security: Nexign outlines the process of responding to security incidents. The data transmission between clients and Nexign is carried out via encrypted channels
- Change Management: Production systems are only changed after proper testing and approval. To maintain a degree of separation between approved and untested releases, distinct environments are implemented: a development environment and a test environment that do not contain real user data, and a production environment. The roles for developing changes, testing, and implementing them in a production environment are segregated.
- Availability: Nexign performs procedures according backup execution and restoring and developed and implemented disaster recovery plan.