SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

# Platform

Relevant to Security

## For the period March 1, 2025 to May 31, 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

# Table of Contents

# 1. Independent Service Auditors' Report

To the Management of Nxtlinq LLC (Nxtlinq)

## Scope

We have examined Nxtlinq's accompanying assertion titled "Assertion of Nxtlinq Management" (assertion) that the controls within Nxtlinq's Platform (system) were effective throughout the period March 1, 2025 to May 31, 2025, to provide reasonable assurance that Nxtlinq's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

## Service Organization's Responsibilities

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

## Service Auditors' 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 AICPA. 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 Nxtlinq'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 Nxtlinq's service commitments and system requirements based on the applicable trust services criteria.

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

## 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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

## Opinion

In our opinion, management's assertion that the controls within Nxtlinq's Platform were effective throughout the period March 1, 2025 to May 31, 2025, to provide reasonable assurance that Nxtlinq's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

San Jose, California

July 14, 2025

# 2. Assertion of Nxtlinq Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Nxtlinq LLC (Nxtlinq) Platform (system) throughout the period March 1, 2025 to May 31, 2025, to provide reasonable assurance that Nxtlinq's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Nxtlinq's Platform," (description) 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 March 1, 2025 to May 31, 2025, to provide reasonable assurance that Nxtlinq's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

Nxtlinq'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 the accompanying system description.

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 March 1, 2025 to May 31, 2025, to provide reasonable assurance that Nxtlinq's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Nxtlinq Management

July 14, 2025

# 3. Description of Nxtlinq's Platform

## Company Background

Nxtlinq is at the forefront of the AI revolution, transforming how enterprises harness data for real-time decision-making. By combining context-aware generative AI and advanced NLP analytics, Nxtlinq enables businesses to extract actionable intelligence from vast, complex datasets—unlocking new opportunities and competitive advantages.

## Services Provided

nxtID

A blockchain-based identity fabric that issues verifiable Human Identity Tokens (HIT) and AI Identity Tokens (AIT) to every user and agent. nxtID ensures that all interactions—whether human or machine-driven—are authenticated, authorized, and fully auditable, delivering end-to-end traceability, dynamic access control, and instant revocation capability without sacrificing user experience.

nxtGPT

An enterprise AI orchestration engine that fan-outs prompts to multiple large-language models, presents side-by-side responses, and lets identity-verified reviewers select and sign their preferred output. Each signed choice becomes a tokenized "preference packet" that powers continuous model improvement via post-training reinforcement and direct preference optimization—turning human judgment into a renewable economic resource.

nxtNLP

A real-time natural-language processing platform that transforms structured and unstructured data into actionable intelligence. Leveraging advanced transformers, sentiment & intent classification, and topic clustering, nxtNLP delivers live pipelines, semantic enrichment, and behavioral signals. Its results feed directly into nxtGPT or downstream analytics, enabling smart routing, compliance checks, and 360° AI-driven decision support.

## Principal Service Commitments and System Requirements

Nxtlinq LLC designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Nxtlinq LLC makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Nxtlinq LLC has established for the services. The system services are subject to the Security commitments established internally for its services.

Nxtlinq's commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Policy, and in the description of the service offering provided online.

# Components of the System

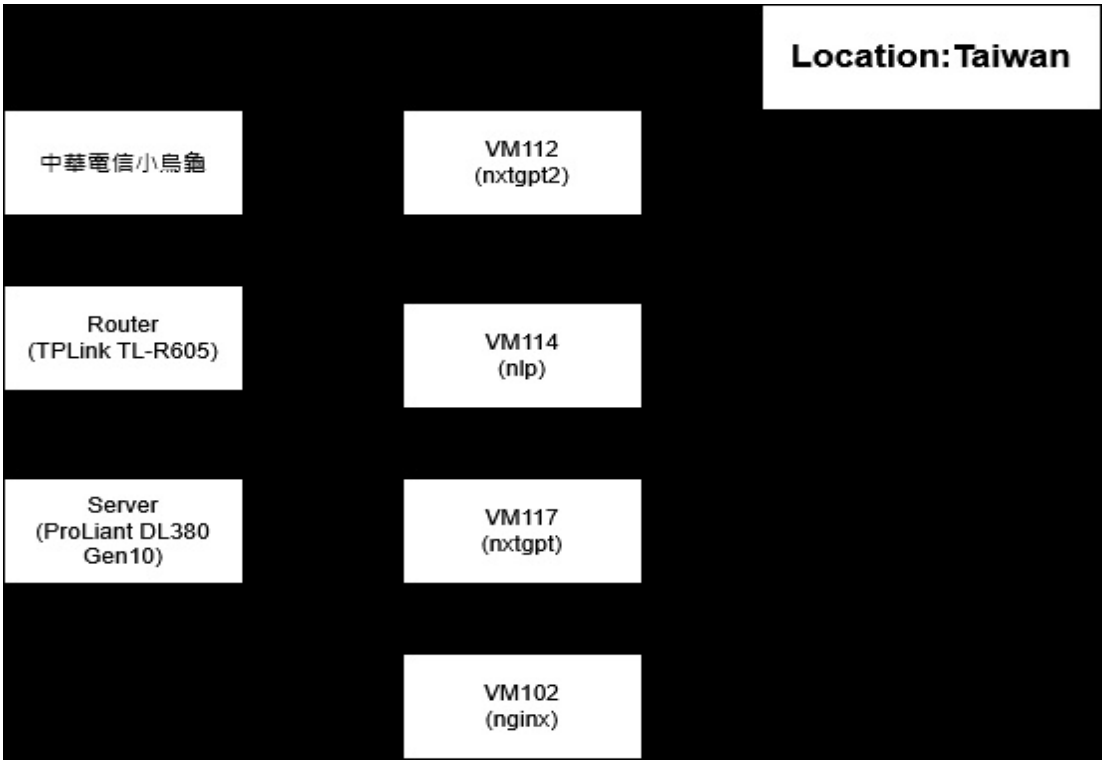
**Components of the system**

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

**Infrastructure**

Nxtlinq LLC maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).



| Hardware | Type | Purpose (optional) |
|---|---|---|
| AWS Elastic Compute Cloud (EC2) | AWS | Resizable compute capacity in the cloud |
| AWS Elastic Load Balancers | AWS | Load balance internal and external traffic |
| Virtual Private Cloud | AWS | Protects the network perimeter and restricts inbound and outbound access |
| S3 Buckets | AWS | Storage, upload and download |
| Azure Platform | Azure | Managed cloud platform where services are hosted |
| Azure Virtual Machine | Azure | Virtual machine service for web hosting and backend service offerings |
| Azure Kubernetes | Azure | Container orchestration for deployment, scaling, and management |
| Azure Database | Azure | Transactional database with backups and redundancy |

**Software**

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

| System/Application | Operating System | Purpose |
|---|---|---|
| GuardDuty | AWS | Security application used for automated intrusion detection (IDS) |
| Datadog | Datadog | Monitoring application used to provide monitoring, alter, and notification services for Nxtlinq LLC platform |
| Azure SDK | N/A | The SDK is used to communicate with Microsoft azure web services |
| Amazon Web Services | N/A | Monitoring and logging |
| Azure DevOps | N/A | Version control |
| Google Workspace | N/A | Identity provider |
| Microsoft Azure | N/A | Monitoring and logging |
| Vanta | N/A | Governance, risk, and compliance management and continuous monitoring |

**People**

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Nxtlinq LLC has a staff organized in the following functional areas:

- Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
- Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.
- Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

**Data**

Data as defined by Nxtlinq LLC, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Nxtlinq LLC:

| Category | Description | Examples |
|---|---|---|
| Public | Public information is not confidential and can be made public without any implications for Nxtlinq LLC. | • Press releases<br>• Public website |
| Internal | Access to internal information is approved by management and is protected from external access. | • Internal memos<br>• Design documents<br>• Product specifications<br>• Correspondences |
| Customer data | Information received from customers for processing or storage by Nxtlinq LLC. Nxtlinq LLC must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information. | • Customer operating data<br>• Customer PII<br>• Customers' customers' PII<br>• Anything subject to a confidentiality agreement with a customer |
| Company data | Information collected and used by Nxtlinq LLC to operate the business. Nxtlinq LLC must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information. | • Legal documents<br>• Contractual agreements<br>• Employee PII<br>• Employee salaries |

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Nxtlinq LLC has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

**Processes, Policies and Procedures**

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

**Physical Security**

Nxtlinq LLC's production servers are maintained by Microsoft Azure and AWS. The physical and environmental security protections are the responsibility of Microsoft Azure and AWS. Nxtlinq LLC reviews the attestation reports and performs a risk analysis of Microsoft Azure and AWS on at least an annual basis.

**Logical Access**

Nxtlinq LLC provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access.

Management is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Nxtlinq LLC's policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 3 business days for that employee's termination.

**Computer Operations – Backups**

Customer data is backed up and monitored by the IT for completion and exceptions. If there is an exception, IT will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in Microsoft Azure and AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

**Computer Operations – Availability**

Nxtlinq LLC maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting and acting upon breaches or other incidents.

Nxtlinq LLC internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Nxtlinq LLC utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

**Change Control**

Nxtlinq LLC maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

**Data Communications**

Nxtlinq LLC has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Nxtlinq LLC application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Nxtlinq LLC uses an automated monitoring service to perform quarterly vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

**Boundaries of the System**

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

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

**The applicable trust services criteria and the related controls:**

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security**: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.

**Control Environment**

Integrity and Ethical Values

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

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

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.

- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

Nxtlinq LLC's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Management's Philosophy and Operating Style

The Nxtlinq LLC management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Nxtlinq LLC can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Nxtlinq LLC to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

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

Nxtlinq LLC's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resource Policies and Practices

Nxtlinq LLC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Nxtlinq LLC's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

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

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

Nxtlinq LLC's risk assessment process identifies and manages risks that could potentially affect Nxtlinq LLC's ability to provide reliable and secure services to our customers. As part of this process, Nxtlinq LLC maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Nxtlinq LLC product development process so they can be dealt with predictably and iteratively.

**Integration with Risk Assessment**

The environment in which the system operates; the commitments, agreements, and responsibilities of Nxtlinq LLC's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Nxtlinq LLC addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Nxtlinq LLC's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communications Systems

Information and communication are an integral component of Nxtlinq LLC's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Nxtlinq LLC uses several information and communication channels internally to share information with management, employees, contractors, and customers. Nxtlinq LLC uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Nxtlinq LLC uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

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

**Ongoing Monitoring**

Nxtlinq LLC's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Nxtlinq LLC's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Nxtlinq LLC's personnel.

### Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

### Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

### Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review date.

### Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Nxtlinq's Platform.

### Subservice Organizations

Nxtlinq's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Nxtlinq's services to be solely achieved by Nxtlinq's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nxtlinq.

The following subservice organization controls should be implemented by AWS & Azure to provide additional assurance that the trust services criteria described within this report are met.

| Security Category | |
|---|---|
| *Criteria* | *Controls expected to be in place* |
| 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. | AWS & Azure are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides. |
| CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users | |

| Security Category | |
|---|---|
| *Criteria* | *Controls expected to be in place* |
| 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. | |
| 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. | |
| 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. | |
| CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | |
| 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. | |
| CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives. | AWS & Azure are responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides. |

Nxtlinq management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Nxtlinq performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

**Complementary User Entity Controls**

Nxtlinq's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Nxtlinq's services to be solely achieved by Nxtlinq's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Nxtlinq's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Nxtlinq.
2. User entities are responsible for notifying Nxtlinq of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Nxtlinq services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Nxtlinq services.
6. User entities are responsible for providing Nxtlinq with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Nxtlinq of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.