Proprietary & Confidential

nintex

System Description of the K2 Cloud Service

SOC 3
Relevant to Security and Availability

FEBRUARY 1, 2022 TO APRIL 30, 2022

MOSSADAMS

Table of Contents

I. Independent Service Auditor's Report

Nintex USA, Inc.
10800 NE 8th St., Suite 400
Bellevue, WA 98004

To the Management of Nintex USA, Inc.:

Scope

We have examined Nintex USA, Inc.'s accompanying assertion in Section II titled "Nintex USA, Inc.'s Assertion" (assertion) that the controls within Nintex USA, Inc.'s K2 Cloud Service (system) were effective throughout the period February 1, 2022 to April 30, 2022, to provide reasonable assurance that Nintex USA, Inc.'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*).

Nintex USA, Inc. uses Microsoft Azure for cloud hosting and identity management (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Nintex USA, Inc.'s controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.'s service commitments and system requirements based on the applicable trust services criteria. 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

Nintex USA, Inc. 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 Nintex USA, Inc.'s service commitments and system requirements were achieved. Nintex USA, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Nintex USA, Inc. 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 (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 Nintex USA, Inc.'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 Nintex USA, Inc.'s service commitments and system requirements based 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 Nintex USA, Inc.'s K2 Cloud Service were effective throughout the period February 1, 2022 to April 30, 2022, to provide reasonable assurance that Nintex USA, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

Seattle, Washington
October 5, 2022

II. Nintex USA, Inc.’s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Nintex USA, Inc.’s K2 Cloud Service (system) throughout the period February 1, 2022 to April 30, 2022 to provide reasonable assurance that Nintex USA, Inc.’s service commitments and system requirements relevant to Security and Availability were achieved. Our description of the boundaries of the system is presented in Section III titled “Nintex USA, Inc.’s Description of the Boundaries of Its K2 Cloud Service” 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 February 1, 2022 to April 30, 2022, to provide reasonable assurance that Nintex USA, Inc.’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)*. Nintex USA, Inc.’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 III titled “Nintex USA, Inc.’s Description of the Boundaries of Its K2 Cloud Service”.

Nintex USA, Inc. uses Microsoft Azure for cloud hosting and identity management (subservice organization). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents the types of complementary subservice organization controls assumed in the design of Nintex USA, Inc.’s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Nintex USA, Inc., to achieve Nintex USA, Inc.’s service commitments and system requirements based on the applicable trust services criteria. The description presents Nintex USA, Inc.’s complementary user entity controls assumed in the design of Nintex USA, Inc.’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 February 1, 2022 to April 30, 2022, to provide reasonable assurance that Nintex USA, Inc.’s service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Nintex USA, Inc.'s Description of the Boundaries of Its K2 Cloud Service

A. System Overview

1. Services Provided

COMPANY BACKGROUND

Nintex USA, Inc. (Nintex or the Company) is headquartered in Bellevue, Washington, with offices in the United States, the United Kingdom, Malaysia, Australia, South Africa, and New Zealand. Nintex strives to make people's jobs easier and their work more productive, from day-to-day tasks to sophisticated business-critical processes. Nintex acquired K2 Software, Inc. in 2021.

K2 Software, Inc. was founded in 1998 in Johannesburg, South Africa, two young software developers had a vision to make process automation easy and change how business was done. Since then, K2 Cloud has grown into a business application software company with five offices and over 500 employees across the globe. The business applications and tools help companies create successful solutions and increase agility. More than 1.5 million users in over 84 countries, including 30 percent of the Fortune 100, are using K2 Cloud to save money, reduce risk, and grow revenue.

DESCRIPTION OF SERVICES PROVIDED

CORE SERVICES

Through the use of the K2 Cloud Service, organizations can build and deploy low-code business applications that are agile, scalable, and reusable, resulting in modern processes that easily connect people, data, decisions, and systems.

K2 Cloud is a cloud-based, Software-as-a-Service (SaaS) offering that provides software and supporting components as a service, in which software and associated maintenance operations can be licensed as a comprehensive service managed by Nintex. Within K2 Cloud, customers are provided:

- *Fully Web-Based Tooling Experience* – Three different persona-based experiences that focus tooling on the specific needs of the customer.
- *Support for Authentication and Authorization* – By integrating into Microsoft Azure Active Directory, customers can utilize their investment in both on-premises and cloud-based identity management.
- *Line-of-Business Integration* – K2 Cloud allows customers to integrate other mission critical applications where business data typically resides, but surface and update that data from applications designed on K2 Cloud, seamlessly combining multiple data sources into a single composite application.

- *Mobile App Platform* – Applications built on K2 Cloud can be surfaced onto leading mobile device platforms so that users can interact with forms and workflows on any screen or experience.
- *Enterprise Workflow Platform* – Providing the abilities to both model and execute enterprise workflow processes that can span groups, users, and systems within an organization.

With the K2 Cloud Service, Nintex provides and maintains the platform that enables customers to build applications on Nintex, without the overhead of setting up, hosting, and maintaining Nintex environments. The customer does not manage or control the underlying infrastructure (such as network, servers, operating systems, storage, or software components), but retains control over the application development cycle and deployed applications.

2. Infrastructure

K2 Cloud Service is based on a multi-tenanted, multi-user software-as-a-service (SaaS), hosted in Microsoft Azure (Azure).

Nintex has outsourced infrastructure resource requirements to Microsoft Azure. Microsoft Azure is a cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed data centers. Microsoft Azure provides SaaS, Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS) services, and supports many different programming languages, tools, and frameworks, including both Microsoft-specific and third-party software and systems. The K2 Cloud Service is built the Microsoft Azure platform and uses many features of Microsoft Azure. New customer instances are created for each customer on the K2 Cloud.

Production servers and client-facing applications are logically and physically separated from Nintex internal corporate information systems. The IT team maintains all internal systems. The Cloud Operations team maintains the production systems in the Microsoft Azure environment.

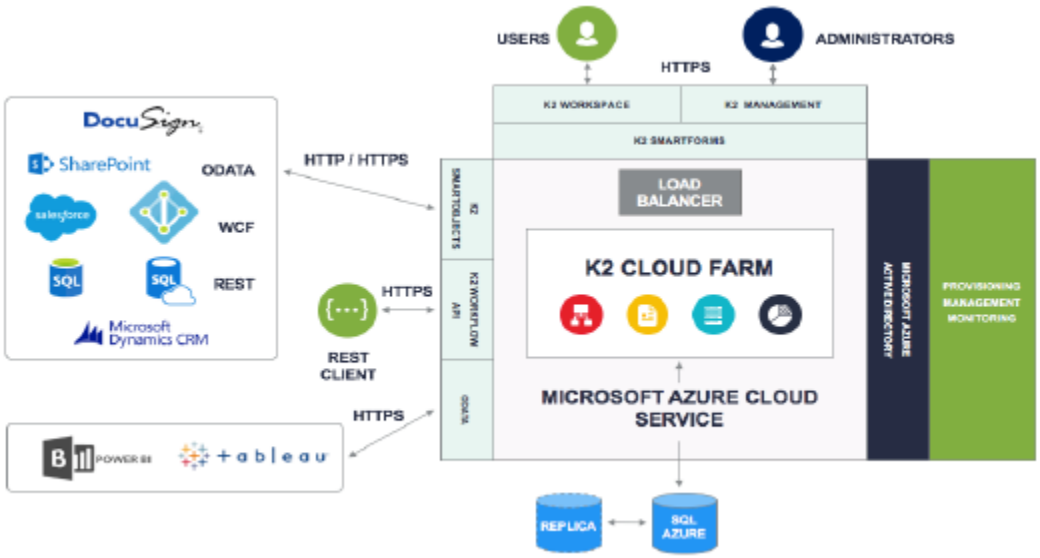

FIGURE 1. HIGH-LEVEL ARCHITECTURE DIAGRAM

3. Software

Nintex Product Teams, incorporating both developers and testers, work together with the Product Management, Quality Assurance, Security, Technical Content, Production Operations, and User Experience and Design Teams to design, develop, and test K2 Cloud. Also, the following third-party applications are utilized to support the production systems:

- *Pingdom* – A service that tracks the uptime, downtime, and performance of the K2 Cloud customer environments and internal IT systems. Pingdom monitors websites from multiple locations so that it can distinguish genuine downtime from routing and access problems and alerts IT personnel as required.
- *Amazon Route 53 DNS* – Highly available and scalable cloud DNS web service. Designed to route end users to K2 Cloud by translating names like kuid.onk2.com into the numeric IP addresses that computers use to connect to each other. Amazon Route 53 DNS effectively connects user requests to infrastructure running in Microsoft Azure.
- *Thycotic Secret Server* – An online password manager. Has multiple layers of built-in security with easy access management for K2 Cloud operations, robust segregation of role-based duties, Advanced Encryption Standard (AES) 256-bit encryption, and out of the box reports to demonstrate compliance.
- *Ticket Management System (TMS)* – Internal ticketing system used by IT and operations personnel for recording security incidents, access requests, and any configuration change management tasks.
- *Landlord* – Software used to orchestrate the K2 Cloud environments' creation, updates, and deletion.
- *BlackOps* – BlackOps fulfills Landlord's requests by making the Application Program Interface (API) calls to third-party providers like Microsoft Azure Domain Name System (DNS), Pingdom, etc.
- *Operations Management Suite* – Cloud-based agent-driven analysis and logging service.

4. People

The Nintex Board of Directors (BOD) reviews the budget and organization structure during the annual business planning meeting. Management reviews budget, organizational reporting lines, and reporting structure in quarterly business reviews. The reporting structure is revised as necessary to address the Company's risk.

Nintex has a staff of over 950 employees organized in the following functional areas:

Staff	
Senior Management Team	Consisting of the Chief Executive Officer (CEO) and other Executive and senior staff responsible for running various functional units below: • CEO • Chief Financial Officer (CFO) • Chief Technology Officer (CTO) • Chief Legal Officer (CLO) and Information Security Officer (ISO) • Chief Customer Officer (CCO) • Chief Product Officer (CPO) • Chief Marketing and Strategy Officer (CMSO) • Chief of Staff • Chief Revenue Officer
Research and Development	Staff responsible for researching and developing key innovations to advance the Nintex platform technologies, including overall product strategy and the development of a product roadmap.
Operations, Practices & Security	Staff responsible for managing operations, security, and quality management.
Customer Success & Support	Staff responsible for providing timely technical support to customers and ensuring customers maintain a positive, productive experience with the Nintex brand.
Marketing	Staff responsible for promoting the Company and communicating a clear, consistent brand across all channels.
Sales	Staff responsible for sales and the development and maintenance of key strategic Nintex partnerships worldwide.
Accounting, Finance, IT, and Human Resources	Staff responsible for managing the fiscal health and day-to-day operations of the Company, including maintenance of corporate resources, and recruitment, training, and retention of staff.

RECRUITING AND TALENT ACQUISITION

Job openings are posted on the Nintex corporate website, as well as on online job sites. Before an offer of employment is made, Nintex conducts interviews and background checks, requiring two or more references and employment verification from the successful candidate's previous employer. Interviews are conducted with one or more members of the relevant team.

ORIENTATION AND PERSONNEL MANAGEMENT

As part of the onboarding program, new employees and contractors are required to review and sign to acknowledge the Employee Handbook. Every employee undergoes annual training on the Nintex security policies and procedures, including physical security, data handling, anti-phishing, and web security.

5. Data

The following table describes the information used and supported by the system:

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer data	Output data is available to customers via the customer K2 Cloud interface.	Confidential

6. Processes and Procedures

Nintex uses security-centric procedures defined in a collection of policy and guideline documents. The Nintex Governance Risk and Compliance (GRC) Team creates and maintains these documents to help employees clearly understand expectations for operating and working at Nintex, including all its products and services. Nintex requires that all employees complete security training on an annual basis, with much of the training content based on the information contained in these policy and guideline documents and the Company's SOC 2 Controls.

Policies	
Access Management Policy	Outlines security practices to prevent unauthorized access to Nintex and customer information systems. This policy defines the rules necessary to achieve this protection and to ensure a secure and reliable operation in accordance with our business requirements, as well as relevant laws and regulations.
Asset Management Policy	Outlines requirements for the identification and protection of physical hardware connected to information systems at Nintex. The level of protection is dependent on the level of classification, its business use, and any applicable regulatory requirements or contractual obligations for those assets.
Information Security Policy	Outlines management direction and support for Information Security Program and Policy activities at Nintex. This policy defines the necessary rules for security protection, and it ensures secure and reliable operations in accordance with our business requirements as well as relevant laws and regulations.
Password Management Policy	Governs password usage of all Nintex employees, contractors, and interns (users). It helps protect Nintex, its users, vendors, partners, and customers from legal liability or other harm due to a compromised network or system.
Patch Management Policy	Outlines the processes to ensure that information systems at Nintex, including applications and software, are patched in a timely manner to reduce or prevent the possibility of unwanted intrusion or exploitation from open vulnerabilities.

Policies	
Security Incident Response Policy	Outlines the requirements for handling a security incident within the Nintex organization. This policy describes appropriate responses to incidents that threaten the confidentiality, integrity, and availability of information assets. Together with the Nintex Security Incident Response Guidelines, this policy establishes an effective incident response program to detect, analyze, prioritize, and handle security incidents.
Vulnerability Management Policy	Outlines scanning processes for scannable endpoint devices. This policy establishes the requirements for scanning, validation of vulnerabilities, and remediation in accordance with the timeframes outlined in the Vulnerability Management and Patch Management Guidelines.

Guidelines	
Account Provision and De-provision Guidelines	Outlines the necessary requirements to create, modify, delete, and maintain user accounts inside the Nintex enterprise environment.
Cryptography Guidelines	Establishes a framework for the proper use of cryptography in Nintex products and services. This guideline informs software development requirements where there may be a choice of implementation functions to use. It covers TLS, symmetric and asymmetric algorithm requirements, and hash function requirements.
Data Handling Guidelines	Establishes a framework for the proper handling of Nintex customer data to ensure data is appropriately handled based on the level of sensitivity, value, and criticality to Nintex.
Enterprise Change Management Guidelines	Provides direction and support for performing production change activities in a consistent manner, including requesting, analyzing, approving, developing, implementing, and reviewing a planned or unplanned change.
Password Guidelines	Provides the framework for how Nintex employees should create, rotate, and protect passwords for Nintex information systems.
Release Management Guidelines	Provides guidance regarding release management for Nintex and supports the Nintex mission to address the needs of its customers and users. These guidelines define requirements for planning, including contingency and rollback planning, releases versus launches, release management checklists, and communications.
Secure SDLC Guidelines	Provides a framework for the SDLC at Nintex. It assists with the identification and mitigation of vulnerabilities.

Guidelines	
Security Incident Response Plan	Provides a framework for the Nintex incident response process for security incidents to inform employees on the standard operating procedures during a security incident.
Security Logging and Monitoring Guidelines	Provides information for logging and monitoring activities on Nintex enterprise information systems and guidance on the security controls to consistently fulfill these requirements.
Vendor Management Guidelines	Provides the procedures for managing Nintex vendor procurement and review lifecycle. This ensures that Nintex obtains the best value for a product or service while controlling exposure to vendor-related risk.
Vulnerability Management Guidelines	Provides a framework for vulnerability management at Nintex, ensuring that Nintex has baseline security across all enterprise information systems where Nintex data may be stored.

SECURITY AND COMPLIANCE

Under the guidance of the Nintex Information Security Practice Team (InfoSec Team), the Development and Production Operations Teams document processes and procedures to support secure development, maintenance, and production of Nintex products and services.

These documents may include:

- Incident response runbooks
- Test plans and test cases
- Operations and productions support procedures
- Logging and monitoring plans

PRODUCT RELEASES

All product releases follow a release plan process, which includes identification and management of security issues, quality-assurance processes, such as static code analysis to maintain code integrity, and contingency or rollback procedures for each release. Changes to the production environment follow a change management procedure, including planning and review, implementation testing, and the development of contingency or rollback procedures.

PRODUCT DOCUMENTATION

Product documentation is hosted in a repository, including a list of tasks and activities that are necessary to the project's success, the owners of those tasks, and timelines for completion. Depending on the nature of the project, additional documentation such as deployment plans, design documents, test plans and test cases, and release notes may also be developed.

B. Principal Service Commitments and System Requirements

PRINCIPAL SERVICE COMMITMENTS

Nintex's commitments to its customers are documented and communicated in the Nintex Master Subscription Agreement and the Nintex Privacy and Customer Use Policies. All customers must enter into an agreement with Nintex in order to access the services. The Nintex Master Subscription Agreement and Privacy and Customer Use Policies are accessible through Nintex's website and are updated regularly.

The Online Privacy Policy includes the following commitments:

- Nintex does not solicit, does not require, and directs customers not to disclose to Nintex any sensitive personal data via the website.
- Customer personal data is processed in accordance with applicable data protection and privacy laws.
- Nintex is responsible under the principles for the processing of personal data it receives under Privacy Shield and subsequently transfers to third parties acting as agents on their behalf.

PRINCIPAL SERVICE REQUIREMENTS

Nintex service system requirements are documented and communicated to employees through internal policies, standards, and procedures. These materials are available to all team members and they agree to comply with these materials at the date of hire. The requirements include:

- System access is implemented according to need-to-know, least privilege, and separation of duties.
- System changes are managed according to change control procedures.
- System components are hardened consistent with internal standards.
- Confidential data is encrypted in transit and at rest.
- System components are monitored for security performance.
- Risks are managed and acknowledged by executive leadership.

C. Complementary Subservice Organization Controls

Nintex USA, Inc.'s controls related to the K2 Cloud Service cover only a portion of overall internal control for each user entity of Nintex USA, Inc. It is not feasible for the criteria related to the K2 Cloud Service to be achieved solely by Nintex USA, Inc. Therefore, each user entity's internal controls must be evaluated in conjunction with Nintex USA, Inc.'s controls, taking into account the types of controls expected to be implemented by the subservice organization as described below.

Complementary Subservice Organization Controls	
1	Microsoft Azure is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the K2 Cloud Service reside.
2	Microsoft Azure is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.
3	Microsoft Azure is responsible for ensuring capacity demand controls are in place to meet Nintex's availability commitments and requirements.
4	Microsoft Azure is responsible for ensuring environmental protection controls are in place to meet Nintex's availability commitments and requirements.

D. Complementary User Entity Controls

Nintex USA, Inc.'s K2 Cloud Service was designed under the assumption that certain controls would be implemented by the user entities for whom it provides its K2 Cloud Service. In these situations, the application of specific controls at these user entities is necessary to achieve certain criteria included in this report.

This section describes additional controls that should be in operation at the user entities to complement the controls at Nintex USA, Inc. User auditors should consider whether the following controls have been placed in operation by the user entity.

Each user entity must evaluate its own internal control structure to determine if the identified user entity controls are in place. User entities are responsible for:

Complementary User Entity Controls	
1	Understanding and complying with their contractual obligations to Nintex.
2	Managing the user access controls for provisioning and deprovisioning user accounts. This includes enforcement of password policies, management of shared accounts, and authorization approvals.
3	Restricting administrative privileges to approved need-to-know personnel.
4	Notifying Nintex of changes made to technical or administrative contact information in a timely manner.
5	Designating internal personnel who are authorized to request user additions, deletions, and security level changes.
6	Understanding and defining data storage requirements.

Complementary User Entity Controls	
7	Securely configuring any enterprise file sync and sharing (EFSS) systems or other systems where files are eventually stored.
8	Managing the confidentiality and integrity of the distribution of authentication tokens used to start component workflows.
9	Managing the need-to-know and least privilege when sharing workflows.
10	Securely managing the connectors including confidential management of account credentials, disabling connections no longer required, and managing need-to-know access to shared account information.
11	Protecting endpoints to thwart malicious software from entering the environment.
12	Immediately notifying Nintex of suspected or confirmed information security breaches such as compromised user accounts or passwords.
13	Developing disaster recovery and business continuity plans that address their ability to use or access the system.

MOSSADAMS