Xi Frame

REPORT ON NUTANIX'S XI FRAME SYSTEM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY (SOC 3 REPORT)

FOR THE PERIOD JANUARY 1, 2019 TO AUGUST 31, 2019

THE cadence GROUP

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

Section I – Report of Independent Service Auditors

To: Nutanix, Inc.

Scope

We have examined Nutanix's accompanying assertion titled "Nutanix's Assertion" (assertion) that the controls within Nutanix's Xi Frame system were effective throughout the period January 1, 2019 to August 30, 2019, to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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*).

Service Organization's Responsibilities

Nutanix 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 Nutanix's service commitments and system requirements were achieved. Nutanix has provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Nutanix 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 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 and in accordance with International Standard on Assurance Engagements 3000 (Revised), *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether 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.

THE cadence GROUP

O 801.349.1360
F 866.326.6612

PO Box 711190
Salt Lake City, Utah 84171
www.thecadencegroup.com

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 Nutanix'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 Nutanix'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.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA. We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

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 controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Nutanix's Xi Frame system were effective throughout the period January 1, 2019 to August 30, 2019, to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Cadence Assurance LLC

October 4, 2019
Salt Lake City, Utah

Section II – Nutanix's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within Nutanix's Xi Frame system throughout the period January 1, 2019 to August 30, 2019, to provide reasonable assurance that Nutanix's service commitments and system requirements relevant to security, availability, processing integrity, confidentiality, and privacy were achieved.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2019 to August 30, 2019, to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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). Nutanix'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.

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 January 1, 2019 to August 30, 2019, to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the applicable trust services criteria.

Nutanix, Inc.
October 4, 2019

Section III – Description of Nutanix's Xi Frame system

Company and Product Overview

Founded in 2009, Nutanix provides cloud services that unify IT operations and bring frictionless application mobility across private, public, and distributed cloud environments. Information technology (IT) teams can seamlessly manage applications across public clouds, including Amazon Web Services (AWS), Google Cloud Platform (GCP), and Microsoft Azure (Azure), as well as on-premises clouds with Nutanix Hyperconverged Infrastructure (HCI). In August of 2018, Nutanix acquired Mainframe2, Inc., dba Frame (www.fra.me).

Xi Frame is a desktop-as-a-service (DaaS) solution that enables customers to quickly deliver applications and software-defined workspaces to users leveraging public cloud infrastructure. No new clients, downloads, or plugins are required. Independent software vendors (ISVs) can offer their customers a subscription-based model, similar to a software-as-a-service (SaaS) product, with minimal to zero changes needed to their existing product(s). Customers can integrate with existing IT systems using Xi Frame's APIs, SDKs, and developer tools. Each Xi Frame subsystem - from connection broker to identity management gateway - uses modern, high performance, cloud-native tools. The encrypted Xi Frame protocol guarantees secure communication between the user's device and the cloud workload running the user's applications. The two networks are isolated, and the Xi Frame protocol is the only entity between them.

System Boundaries

The system boundaries for consideration within the scope of this report are the processes, infrastructure, and software that store, access, operate, or transmit user data within the Nutanix Xi Frame system. Specifically, the system environment includes the following:

- A central global platform-as-a-service (PaaS) that provides cloud automation and orchestration to deliver an end-to-end managed DaaS solution
- Dynamic orchestration of virtual desktop and application workload instances
- Management and orchestration of the relevant IaaS provider services and Nutanix Acropolis Hypervisor Virtualization (AHV) / HCI services
- Video delivery and system control channels of workload instances
- Identity and access management solutions for customers

Excluded from the scope of this report:

- Customer user account management (beyond the accurate storage and implementation of configured authorizations)
- Network security on any tunnels configured into/out of the Nutanix Xi Frame workload environment(s) for individual customers

- Security of any workload instances beyond the standard configurations and network layer protections inherent in the IaaS provider selected by the customer and/or their internal network for Nutanix HCI for the given workload instances
- Security of customers Bring Your Own (BYO) cloud accounts

Subservice Organizations

Nutanix Xi Frame uses the following third-party subservice organizations:

- AWS - Provides management and hosting of the production servers and workload instances in an IaaS model.
- Azure - Provides management and hosting of workload instances in an IaaS model.
- GCP - Provides management and hosting of workload instances in an IaaS model.

The scope of this report includes only the controls of Nutanix Xi Frame, and excludes controls that are the responsibility of Amazon, Google, and Microsoft.

Principle Service Commitments and System Requirements

Nutanix designs its processes and procedures related to the Xi Frame system to meet its business objectives. These objectives are based on the service commitments Nutanix makes to customers and other relevant user entities, and the operational and compliance requirements that Nutanix has established for the services. Service commitments to customers and other relevant user entities are documented and communicated in master agreements and supplemental terms agreements, as well as in the description of the service offering provided on Nutanix's website, in their marketing materials, and within their customer-facing web portal.

Nutanix has established operational, development, and engineering requirements that support the achievement of security commitments against its products. Such requirements are communicated via Nutanix's system policies and procedures, system design documentation, and contracts with customers. Information security (IS) policies define an organization-wide approach to how systems and data are protected. These policies include how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required for the ongoing development and operation of the Xi Frame system.

System Components

The following section outlines the system components that make up the Xi Frame system.

Infrastructure

The core Nutanix Xi Frame applications run on a mix of AWS infrastructure as a service (IaaS) and AWS platform as a service (PaaS). Workloads can run in AWS, Azure, or GCP regions or on Nutanix HCI within customer data centers.

Software

The Nutanix Xi Frame as a service architecture consists of a set of core components that provide user and administrator user interfaces (UIs), orchestration of Infrastructure as a Service (IaaS) provider resources and Nutanix HCI resources for on-premises implementations, user authentication/authorization, end user session remoting protocol, and usage tracking. The platform is deployed on the AWS infrastructure in its own Virtual Private Cloud (VPC) and includes the following components:

- Dashboard (CPanel)
- Launchpad
- Gateway
- Identity Management Gateway (IMG)
- Nutanix Xi Frame Guest Agent (Formerly Frame Server)
- Terminal
- Nutanix Xi Frame Meter
- Nutanix Cloud Connector

People

Nutanix Xi Frame employees involved in the definition, development, operation, or support of the core Nutanix Xi Frame are grouped into five primary areas: Security and Compliance, Engineering and Operations, Business Operations, Sales, and Customer Success.

Procedures

Nutanix Xi Frame has an established information security program managed by the Senior Director of Security. Nutanix Xi Frame establishes and maintains formal policies and procedures to delineate standards for logical access on the provider platform(s) and virtual hosts. The policies also identify functional responsibilities for the administration of logical access and security.

Policies and procedures, including those related to security, user access, and change management, have been created and made available for Nutanix personnel through the intranet. Each policy is assigned an owner, and is reviewed and updated at least annually, or as necessitated by process changes. Additionally, a disaster recovery policy is established that includes procedures related to backup, replication, and recovery activities. Documentation is maintained to aid and inform operations personnel in handling incidents or issues. If the resolution of an issue requires collaboration, operational personnel use a conferencing system to support communication, progress updates, and logging capabilities. Post-mortem discussions are convened after any significant operational issue, regardless of external impact. Further, incident reports capture the root cause of the incident and preventative actions to help prevent future occurrences of the incident. Implementation of the preventative measures is tracked during weekly Product Management meetings.

Data

Customer data on the Nutanix Xi Frame or in the workload VMs remains the sole property of Nutanix Xi Frame's customers. Customer data is stored in customer on-premises storage via VPN, customer-selected cloud storage, or customer-managed file servers. If the customer application requires a database server (e.g., client-server application), the customer is responsible for implementing and managing their own database server. The type of data stored in these databases is determined by the customer and the type of application being used. Customer data stored on internal Nutanix Xi Frame systems is limited to system metadata, session telemetry, system configurations, login events, authorization, and general usage information of the Nutanix Xi Frame.

- Session metadata simply refers to the collection of details that are captured when various operations are performed within the Frame environment. Organizations use this data to identify users, session start times and durations, instance type used, session type (desktop or published applications), published applications used, as well as other operational details.
- Session telemetry refers to the transmission and measurement of data between the end user's browser and the Frame workload virtual machine. Organizations use this data to evaluate the session performance and quality of the experience for the end-user.

Internal Control Framework

The following section describes the aspects of Nutanix's internal control environment.

Control Environment

A company's internal control environment reflects the overall attitude, awareness, and actions of executive management, the board of directors, and other stakeholders concerning the importance of controls and the emphasis given to controls in the company's policies, procedures, methods, and organizational structure. The following is a description of the control environment as it pertains to Xi Frame.

Nutanix management is responsible for directing and controlling operations and for establishing, communicating, and monitoring policies and procedures. Importance is placed on maintaining sound internal controls and establishing the integrity and ethical values of personnel.

Risk Assessment

An entity's risk assessment process is its identification, analysis, and management of risks and its service delivery to user organizations. Nutanix recognizes that risk management is a critical component of its operations that helps to verify that customer assets are properly protected.

Management is responsible for identifying the risks inherent in the company's operations and for implementing procedures and controls to monitor and mitigate these risks. The foundation of this process is management's knowledge of its operations, its close working relationship with its customers and vendors, and its understanding of the cloud space in which it operates. Management meets monthly to discuss changes to the risk landscape, including risks related to security, availability, and confidentiality. Based on these discussions, management takes actions to update the risk register, procedures, and controls to monitor and mitigate risk.

Control Activities

Controls have been implemented to address system and data risks. Controls have been designed and implemented in the following areas:

- Account Provisioning
- Periodic Account Review
- Access Removal
- Customer Data Retention and Destruction
- Access to Customer Data
- Password Policy
- Incident Response
- System Monitoring

- Endpoint Security
- Encryption
- Asset Management
- Logical Security
- Vulnerability Management
- Change Management
- Backup and Availability

Information and Communication

To help align Nutanix business strategies and goals with operating performance, management is committed to maintaining effective communication with employees and customers.

Nutanix maintains security standards and procedure documentation for employees. Changes and updates to security policies are communicated to employees through company-wide email and through annual security training. New employees are briefed on Nutanix's security policy during employee orientation and each employee acknowledges the policies in place during orientation and annually thereafter.

Xi Frame maintains several channels of customer communication depending on the type of communication required. These channels include customer support (available via phone, email, and web forms), a web page (http://status.fra.me), an email distribution list, and personal contacts with Xi Frame account managers. Inbound questions, issues, or similar are supported via the customer support channels or directly to account managers. After hours, critical support issues go through the customer support channels. System status updates are posted on status.fra.me and sent to the email distribution list. Communication, including the transfer of customer data and web portal transactions, is encrypted.

Customers are provided with information necessary to use the Nutanix services through the online terms of service. Customer contracts include a description of the services, system availability, system boundaries, support functions, and responsibilities of the customer and Nutanix.

Enhancements and defect fixes applied to the Xi Frame system are posted to the online change log at https://docs.frame.nutanix.com.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in conditions. Management and supervisory personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. To complement these measures, exceptions to normal or scheduled processing is logged, reported, and tracked until resolved. Additionally, root cause analysis is performed on significant incidents to ensure they are not repeated.

The Compliance team performs an annual assessment over internal controls used in the achievement of Xi Frame's service commitments and system requirements. Significant findings are shared with senior management for evaluation and resolution.

Complementary User Entity Controls

Nutanix's controls were designed under the assumption that certain controls would be implemented by user organizations, the application of which is necessary to meet certain trust services criteria identified in this report. This section highlights those internal control responsibilities Nutanix believes should be present at each customer, and has considered in developing its controls reported herein. Nutanix customers should evaluate their own control environment to assess if the following controls are implemented and operating effectively. These complementary user entity controls do not represent a comprehensive list of controls that should be employed by Nutanix customers, but provide a summary of controls necessary to meet the stated trust services criteria presented in this report. These controls include the following:

- Customers are responsible for setting password requirements and multi-factor requirements for their SSO authentication solution.
- Customers are responsible for security and user administration to their portal including: user provisioning, de-provisioning, and authorization to protected resources, such as Control Panel, Dashboard, Launchpad, and different administrator levels.
- Customers are responsible for secure configuration and operations when they leverage their own AWS, Azure, and GCP IaaS accounts and Nutanix HCI on-premises with the Nutanix Xi Frame.
- Customers are responsible for the deletion of instances when they leverage their own AWS, Azure, and GCP IaaS accounts and Nutanix HCI on-premises within the Xi Frame.

Complementary Subservice Organization Controls

Nutanix contracts with AWS, Azure, and GCP for hosting the production environment used to provide the cloud hosted system. Controls managed by these third-party subservice providers are not included in the scope of this report. Expected subservice provider controls that have an effect on specific criteria are included below.

Criteria	Expected Controls
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.	Access to hosted systems requires users to use a secure method to authenticate. User content is segregated and made viewable only to authorized individuals. Network security mechanisms restrict external access to the production environment.
CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	New user accounts are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
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.	Access modifications to hosted systems are approved by appropriate individuals prior to being provisioned. User accounts are removed when access is no longer needed. User accounts are reviewed on a regular basis by appropriate personnel.
CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Access to physical facilities is restricted to authorized users.

Criteria	Expected Controls
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.	Production media is securely decommissioned and physically destroyed prior to being removed from the data center.
CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Network security mechanisms restrict external access to the production environment. Encrypted communication is required for connections to the production system.
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.	Access to hosted data is restricted to appropriate users. Hosted data is protected during transmission through encryption and secure protocols.
CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus or antimalware solutions are installed to detect or prevent unauthorized or malicious software.
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	System configurations changes are logged and monitored. Vulnerabilities are identified and tracked to resolution.
CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Security events are monitored and evaluated to determine potential impact per policy.

Criteria	Expected Controls
CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Operations personnel log, monitor and evaluate to incident events identified by monitoring systems
CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Operations personnel respond, contain and remediate incident events, and update stakeholders, as needed.
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	System changes are documented, tested, and approved prior to migration to production. Access to make system changes is restricted to appropriate personnel.
A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Operations personnel monitor processing and system capacity.
A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Environmental controls protect the physical devices supporting the production environment.
A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.	System failover and backup procedures are tested.