NorthCapital

SOC 3® Report

Controls Related to Security

For the Period April 15, 2024 to April 14, 2025

Prepared in accordance with the attestation standards established by the American Institute of Certified Public Accountants

mjd ADVISORS

Table of Contents

Independent Service Auditor's Report

To the Management of North Capital Investment Technology, Inc.
Midvale, Utah

Scope

We have examined North Capital Investment Technology, Inc.'s (the Company) accompanying assertion titled "Assertion of North Capital Investment Technology, Inc.'s Management" (assertion) that the controls within the North Capital Platform (the Platform) were effective throughout the period April 15, 2024 to April 14, 2025, to provide reasonable assurance that the Company'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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

The Company is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the Platform to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled "Assertion of North Capital Investment Technology, Inc. Management" about the effectiveness of controls within the Platform. When preparing its assertion, the Company 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 Platform.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that the controls within the Platform were effective throughout the period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted following 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 the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion. We are required to be independent of the Company and to meet our other responsibilities in accordance with relevant ethical requirements relating to the engagement.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

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

Inherent Limitations

There are inherent limitations in 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 suitability of the design or operating 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 the Platform were effective throughout the period April 15, 2024 to April 14, 2025, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, is fairly stated, in all material respects.

MJD Advisors

Waukee, Iowa
January 7, 2026

Assertion of North Capital Investment Technology, Inc. Management

We, as management of North Capital Investment Technology, Inc., are responsible for designing, implementing, operating, and maintaining effective controls within the Platform throughout the period April 15, 2024 to April 14, 2025, to provide reasonable assurance that the Company's service commitments and system requirements relevant to security were achieved. We have described the boundaries of the Platform in the section titled "Management's System Disclosures" (the System Disclosures), which identifies the aspects of the Platform covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the Platform throughout the period April 15, 2024 to April 14, 2025, to provide reasonable assurance that the Company'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* (AICPA, *Trust Services Criteria*).

Our objectives for the Platform in applying the applicable trust services criteria are embodied in our 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 System Disclosures.

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 Platform were effective throughout the period April 15, 2024 to April 14, 2025, to provide reasonable assurance that our service commitments and system requirements were achieved based on the applicable trust services criteria.

Management of North Capital Investment Technology, Inc.
January 7, 2026

Management's System Disclosures

Types of Services Provided

North Capital Investment Technology, Inc. is responsible for the development and maintenance of the North Capital Platform, TransactCloud (the Platform). The Company is the parent company of its wholly owned subsidiaries North Capital Inc. and North Capital Private Securities Corporation, which provide services as a registered investment advisor and registered broker-dealer, respectively. These services are not within the scope of this description, except for any information stored and processed by the Platform in connection with these services.

The Platform provides a suite of technology-based investment solutions to broker-dealers, banks, fund managers, funding platforms, and private issuers who wish to access private investment markets. The specific products within the scope of this description include the following:

TransactAPI: Transactional technology platform that enables broker-dealers, funding platforms, and issuers to conduct online private securities offerings. The system is accessible through a standards-based API toolkit that can be tailored to the needs of the sponsor and provides automation to meet KYC, AML, suitability screening, and accredited investor verification requirements, accept funds via ACH, credit card, check, or wire transfer, and facilitate document exchange and electronic signature.

Other related sub-products within the TransactAPI include:

- **DirectInvest Button:** Single-offering module intended for individual issuers, offering similar functionality as TransactAPI, that can be embedded on a website, within an iframe, or shared as a URL and facilitates the complete investment process for the investor.
- **Marketplace-as-a-Service:** Integrates the capability of TransactAPI as a white-label solution that incorporates a customer's logo and branding and provides additional customization.
- **Direct Accreditation Button:** Automates the investor verification process through a micro portal placed on a web page or Reg D offering to meet KYC, AML, and accredited investor verification requirements.
- **PPEX ATS:** Provides for electronic order matching of buy and sell orders through TransactAPI functions.
- **OPERA:** Provides a multi-tenant platform integrating the capability of TransactAPI as a white-label platform solution for issuers, managers, and marketplace sponsors. OPERA is scheduled to replace DirectInvest Button, Marketplace-as-a-Service, and Direct Accreditation Button as they reach end of life.
- **BARC:** The company's books and records and internal compliance system, parts of which are accessible to customers.

Boundaries of the Platform

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The boundaries of the system described in this description include the system components related to the service life cycle, such as initiation, authorization, processing, recording, and reporting for the services provided to user entities. The system boundaries do not include instances in which transaction-processing information is combined with other information for secondary purposes internal to the service organization, such as accounting and billing.

Infrastructure

The Company leverages the experience and resources of Amazon Web Services (AWS) to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the Platform architecture within the cloud hosting environment to ensure security and resiliency requirements are met.

The specific services utilized to support the Platform's cloud infrastructure include the following:

Cloud Hosting Services	
Service	**Description**
Amazon ECR	Managed container registry
AWS Fargate	Serverless compute engine for containers
Amazon API Gateway	Managed API service
Amazon Athena	Query service
AWS WAF	Web application firewall
Amazon Eventbridge	Serverless event bus
Amazon ElastiCache	Managed caching service
Amazon Aurora	Managed relational database management system
Amazon RDS	Managed relational database service
AWS CodeBuild	Managed continuous integration service
AWS CodeDeploy	Managed deployment service
AWS CodePipeline	Managed continuous delivery service
AWS Config	Monitors, records, and evaluates AWS resource configurations
AWS Certificate Manager	Encryption certificate management service
AWS Secrets Manager	Manages API keys, OAuth tokens, and other secrets
AWS Trusted Advisor	Monitoring for AWS best practices for security and performance
Amazon Inspector	Security assessment and vulnerability management service
Amazon GuardDuty	Threat detection service

Cloud Hosting Services	
Service	**Description**
Amazon CloudWatch	Infrastructure resource and application monitoring
AWS CloudTrail	Infrastructure audit logging
AWS Elastic Compute Cloud	Compute service
AWS Lambda	Serverless, event-driven, compute service
AWS S3	Object storage
AWS Elastic Load Balancer	Distributes network traffic across available resources
AWS ECS	Managed container service
AWS Virtual Private Cloud	Provides a logically isolated virtual network that uses network security groups to control traffic

Certain controls of AWS are necessary in combination with the Company's controls to provide reasonable assurance that the Company's service commitments and system requirements are achieved based on the trust services criteria (Complementary Controls). The Company is responsible for the oversight and monitoring of AWS, which is performed through the vendor management policies and procedures.

The following are the applicable trust services criteria and controls that are necessary to be in place at AWS to provide reasonable assurance that the Company's service commitments and system requirements were achieved:

Complementary Controls	
Criteria	**Control**
Logical and Physical Access CC6 Series	Procedures are implemented to authenticate authorized users, restrict physical and logical access, and detect unauthorized access attempts and procedures are implemented to decommission and physically destroy production assets securely. Security measures are implemented to provision and deprovision user access to systems and applications based on appropriate authorization, and encryption has been implemented, by default or as configured by the Company, to secure the transmission and storage of information.
System Operations CC7 Series	Vulnerability scans and penetration testing are performed periodically to identify system vulnerabilities, and environmental protection, monitoring, and procedures for regular maintenance are implemented at the data center facilities. Incident response procedures are established and implemented to identify, analyze, and remediate events and incidents.

Complementary Controls	
Criteria	**Control**
Change Management CC8 Series	Procedures are established and implemented to ensure system changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.

The examination performed by the independent service auditor did not extend to the policies, procedures, and controls of AWS.

Software

Software consists of the programs and software that support the Platform. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Platform includes the following:

Software Summary	
Application	**Purpose**
OneTrust	Compliance management platform
GitHub	Source code repository
Google Workspace	File storage, email, document collaboration, identity provider
Slack	Communication hub
HubSpot	Customer relationship management
ZAP	Web application vulnerability scanning
Slab	Communication and knowledge sharing
Jira, Trello	Project management and issue tracking

Product Integrations

The Company leverages the resources and experience of third-party services that are integrated with the Platform (Product Integrations) to enhance the user experience and allow developers to focus on the core product offering. These integrated service offerings are subject to the Company's vendor management policies and have been selected based on their status as industry leaders in each required domain. Management evaluates the services provided and the risk of each provider to determine due diligence procedures, monitoring, and other controls to be implemented.

The specific services provided through integrations with third parties include the following:

Production Integrations Summary	
Service	**Description**
Plaid	Plaid is a financial services company that builds a data transfer network to power fintech and digital finance products. Its product, a technology platform, enables applications to connect with users' bank accounts.
Stripe	Stripe is a suite of APIs powering online payment processing and commerce solutions for internet businesses of all sizes.
DeliverySlip	DeliverySlip is an email management solution that helps businesses in legal, financial, and other industries handle customer communication, online campaigns, and data-sharing operations.
IDology	IDology is a global provider of Identity Verification and Document Authentication solutions to fight fraud and maintain KYC compliance.
LexisNexis	LexisNexis is a consumer reporting agency that provides information about individuals that commercial organizations, government agencies, and nonprofits need to get a complete picture of individuals, businesses, and assets.

People

The Company's organizational structure provides the framework for the management, operation, and security of the Platform. The table below summarizes the key roles and functional responsibilities of the Company. Due to the Company's size, one individual may serve multiple roles.

Organizational Structure	
Role	**Function**
Board of Directors	Responsible for governance, oversight of management, and major decision making, representing the interests of shareholders and includes members independent of management
CEO	Responsible for oversight of the development and performance of internal controls and the direction of company-wide activities
CISO & CTO	Together with the Chief Technology Officer, responsible for the design, development, maintenance, dissemination, and enforcement of the Information Security Program
Security Operations Team	Cross-functional team responsible for oversight, implementation, and continual improvement of the Information Security Program
Business Operations	Manages internal business needs such as human resources, customer success, and other administrative functions

Organizational Structure	
Role	**Function**
Legal	Responsible for compliance and legal functions of the Company, including external attorneys providing services under management supervision
Engineering Team	Responsible for the development, testing, deployment, and maintenance of the Platform and for maintaining security
Outsourced Development	Third-party development agency (EphronTech) responsible for supporting the development and maintenance of the Platform at the direction of the Company's personnel
Risk Committee	Provide oversight of compliance and risk management activities with respect to due diligence related to customers, vendors, and regulatory requirements
Compliance	Responsible for the compliance functions of the Company

Procedures

Procedures are the specific actions undertaken to implement a process, consisting of linked procedures designed to accomplish a particular goal. Policies, which serve as the basis of procedures, are management's statements of what should be done to meet system objectives and may be documented, explicitly stated in communications, or implied through actions and decisions. The Company has adopted the following defined set of information security standards and policies:

- Acceptable Use Policy
- Backup and Restoration Policy
- Change Management Policy
- Data Retention and Disposal Policy
- Information Classification Policy
- Personnel Security Policy
- Server Security Policy
- Software Development Policy
- Workstation and Mobile Devices Policy
- Vulnerability and Penetration Testing Policy
- Access Control Policy
- Corporate Ethics
- Incident Management Policy
- Information Security Policy
- Network Security Policy
- Risk Assessment Policy
- Serverless Security Policy
- Vendor Management Policy
- Key Management and Cryptography Policy
- Business Continuity and Disaster Recovery Policy

Data

Data refers to the transaction streams, files, data stores, tables, and output used or processed by the Company. Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established with customers and business partners. The following table details the types of data collected by the Company in connection with the Platform's services and the infrastructure, software, and third-party vendors utilized to store and process the data.

Data Type Summary		
Type	**Description**	**Storage and Processing**
Account data	Personally Identifiable Information and other administrative data from personnel, customers, and other third parties	AWS and other third-party managed applications
Customer data	Confidential information stored and processed on behalf of customers in connection with services provided by the Platform.	AWS
Secrets	Access credentials, tokens, certificates, API keys, and other secrets	AWS Secrets Manager, AWS Certificate Manager, AWS Config
Log information	Information relevant to and explicitly necessary for services, including metadata	AWS CloudTrail, Amazon CloudWatch

Principal Service Commitments and System Requirements

The information presented within the Boundaries of the Platform was prepared to describe the procedures and controls the Company implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the critical objectives that drive the system's operation.

System Requirements

The Company's system requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures have been prepared to describe specific manual and automated processes required to operate and develop services provided.

Service Commitments

Service commitments include those made to user entities and others (such as customers of user entities) to the extent those commitments relate to the trust services category or categories addressed by the description. Security objectives and commitments are made available to customers through software and services license agreements, and information shared on the Company's website. The following summarizes the Company’s principal service commitments that management believes to be relevant to the report users:

- The Company uses commercially reasonable physical, managerial, and technical safeguards designed to secure data from accidental loss and unauthorized access.
- Customer data is encrypted at rest and in transit.
- Access to critical resources and sensitive information requires multi-factor authentication and is provided based on the principle of least privilege.
- The Company continuously monitors access to its infrastructure.
- IP whitelisting is offered as a recommended option for end-user organizations.