DIGITAL CHECK CORP. AND ITS SUBSIDIARIES AVIVATECH LLC AND BENCHMARK TECHNOLOGY GROUP, INC.

Software Services

SOC 3

System and Organization Controls (SOC) for Service Organizations Report
for the period of May 1, 2024 to May 2, 2025

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor 1

II. Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s Assertion 4

III. Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s Description of the Boundaries of its System 6

A. Scope and Purpose of the Report 6

B. Company Overview and Background 6

C. System Overview 6

D. Principal Service Commitments and System Requirements 11

E. Subservice Organizations 12

F. User Entity Responsibilities 15

I. Report of Independent Service Auditor

We have examined Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s (the "Company") accompanying assertion titled Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s *Assertion* (the "Assertion") indicating that the controls within the Software Services (the "System") were effective for the period of May 1, 2024 to May 2, 2025 (the "Specified Period") to provide reasonable assurance that Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality ("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) (AICPA, Trust Services Criteria) for the Specified Period.

The Company uses Google Cloud Platform (GCP) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses Google Filestore and Google BigQuery as a Platform-as-a-Service. The Company also uses Microsoft Azure (Azure), a subservice organization, for its Software-as-a-Service Entra ID Domain Services (Azure Entra ID DS). Additionally, the Company uses Meridian IT, Inc. (Meridian), a subservice organization, for its backup monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. Lastly, the Company uses Amazon Web Services (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. Certain AICPA applicable trust services criteria specified in the section titled *Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's Assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. The Assertion does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's responsibilities

The Company 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 the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company 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 the controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our qualified opinion.

We are required to be independent and to meet our ethical 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 controls were not effective to achieve the Company'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 the Company's service commitments and system requirements based on the applicable trust services criteria;
- performing procedures to obtain evidence about whether controls were suitably designed and operating effectively to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- testing the operating effectiveness of controls to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.

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

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 issued by the International Ethics Standards Board for Accountants (IESBA Code). We have applied the Statements on Quality Control Standards established by the AICPA and, accordingly, have designed, implemented, and operate a system of quality management including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

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.

Other matters

We did not perform any procedures and accordingly do not express an opinion on the description in Section III titled *Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s Description of the Boundaries of its System.*

Basis for Qualified Opinion

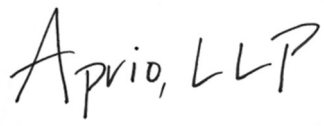
The Company has not implemented controls to address the risk that DevOps management personnel are alerted when changes are implemented to the packaged build folder for Microfilm Solutions (i.e., nextStarPLUS and PerfectView). In addition, evidence of the completion of the peer review prior to promotion into the production environment was not properly documented for Microfilm Solutions. As a result, controls were not suitably designed or operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the following trust services criteria:

- Common Criteria CC 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
- Common Criteria CC 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Qualified Opinion

In our opinion, except for the effects of the matters referred to in the preceding paragraph, in all material respects, Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s assertion that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria , in all material respects, is fairly stated.

Aprio, LLP



Atlanta, Georgia
June 18, 2025

The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

II. Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s (the "Company") Software Services (the "System") for the period of May 1, 2024 to May 2, 2025 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (the "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) (AICPA, *Trust Services Criteria*). The Company'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. Our description of the boundaries of the system and principal service commitments and system requirements related to the applicable trust services criteria are specified in the section titled Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s *Description of the Boundaries of its System*.

The Company uses Google Cloud Platform (GCP) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses Google Filestore and Google BigQuery as a Platform-as-a-Service. The Company also uses Microsoft Azure (Azure), a subservice organization, for its Software-as-a-Service Entra ID Domain Services (Azure Entra ID DS). Additionally, the Company uses Meridian IT, Inc. (Meridian), a subservice organization, for its backup monitoring services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. Lastly, the Company uses Amazon Web Services (AWS), a subservice organization, Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. Certain AICPA applicable trust services criteria specified in the section titled Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s *Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations.

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.

Except for the matter described in the paragraph below, we assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria.

The Company has not implemented controls to address the risk that DevOps management personnel are alerted when changes are implemented to the packaged build folder for Microfilm Solutions (i.e., nextStarPLUS and PerfectView). In addition, evidence of the completion of the peer review prior to promotion into the production environment was not properly documented for Microfilm Solutions. As a result, controls were not suitably designed or operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the following trust services criteria:

- Common Criteria CC 6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
- Common Criteria CC 8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

III. Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of Digital Check Corp. and its Subsidiaries Avivatech LLC and Benchmark Technology Group, Inc.'s (the "Company") as it relates to its Software Services (the "System") for the period of May 1, 2024 to May 2, 2025 (the "Specified Period"), for the trust services criteria relevant to Security, Availability, and Confidentiality (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (With Revised Points of Focus – 2022) (AICPA, *Trust Services Criteria*).

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

The Company is comprised of several business units: (i) "Avivatech", its cash and check automation software business; (ii) "Benchmark", its reseller and fulfilment business; (iii) "Digital Check", its check scanner business; (iv) "ST Imaging", its microfilm and microfiche reader business; and (v) "nextScan", its microfilm and microfiche conversion business. ST Imaging and nextScan share personnel and principal operations in Meridian, Idaho, and therefore are often referred to collectively as "DC Idaho" or "DCI".

Avivatech provides software that delivers cash automation efficiency, image enhancement, and deposit-processing technologies that help clients reduce costs and improve their cash and check workflows. Avivatech also offers professional services related to its solutions.

Benchmark resells hardware and software commonly used in bank branches, including Digital Check scanners, Avivatech software, and third-party equipment. Benchmark also provides fulfillment, installation, conversion, and support of both Avivatech software solutions and third-party hardware that is resold by Benchmark and others.

Digital Check manufactures check scanners and provides check scanners, peripherals, and related solutions for the banking industry.

ST Imaging manufactures micrographic reading equipment and provides related software and solutions.

nextScan manufactures micrographic scanning and conversion equipment and provides related software and solutions.

C. System Overview

Supporting Systems Overview

The Company provides check and cash solutions for banking and retail customers. Microfilm and microfiche conversion and microfilm and microfiche reader solutions are provided to service bureaus, educational institutions, insurance agencies, and government entities, among others.

TraxIT is developed and hosted by Benchmark out of its Alpharetta, GA location. XpressControl is developed and hosted by Avivatech within a Google Cloud Platform (GCP) Cloud Environment. All other applications listed below during the Specified Period were operated from the customers' environments.

XpressScan is developed by Avivatech, and the development environment is housed within an Amazon Web Services (AWS) Cloud Environment. The production instance of XpressScan is housed within the customers' environment, as such, the XpressScan development environment was the only environment of the AWS environment that was in-scope of for this report.

Banking Solutions:

- autoMICR
- CashWare
- QDS Capture
- TraxIT
- Vault by Avivatech
- Clear by Avivatech

Retail Solutions:

- XpressCash
- XpressScan
- XpressControl

Microfilm Solutions

- nextStarPLUS
- PerfectView

Application Name	Software Details

CashWare	• Architecture: .NET thick client application.
	• Application Description: Application designed to interface with cash handling peripherals such as Cash Recyclers or Coin Recyclers. The target market are banks/financial institutions.
	• OS – Windows
	• Server Dependencies
	  ○ None
	• Software Dependencies
	  ○ SQL Server Express

XpressControl	• Architecture: Web-based application written in NodeJS
	• Application Description: XpressControl is a web application that allows retailers to track cash transactions across all channels in their enterprise. The target market is retail.
	• OS – Windows
	• Server Dependencies
	  ○ NodeJS
	  ○ PM2
	• Software Dependencies
	  ○ Browser

XpressScan	• Architecture: Web-based application written in PHP • Application Description: XpressScan is a web application that allows retailers to scan checks at the retail location directly and electronically post the information to their bank of choice. Digital Check Scanners may be used as the scanning hardware. The target market is retail. • OS – Windows

Application Name	Software Details
	• Server Dependencies • IIS • .NET / C++ / PHP • Software Dependencies • Browser

XpressCash	• Architecture: .NET thick client application written in C#.
	• Application Description: Application designed to interface with cash handling peripherals such as cash recyclers or coin recyclers. The target market are retailers.
	• OS – Windows
	• Server Dependencies
	  ○ None
	• Software Dependencies
	  ○ SQL Server Express

Clear by Avivatech	• Architecture: thick client application written in C++ and C# • Application Description: a stand-alone check scanner capture windows application used to scan items that were bad or non-conforming images (NCI) from the bank's various processing department. • OS - Windows • Server Dependencies • IIS • C++ /C#/ PHP • Software Dependencies • Chrome Browser • Hardware Dependencies • Digital Check check scanner (TS240, cx30)
Vault by Avivatech	• Architecture: Web-based application written in NodeJS • Application Description: Works with multi-customer and multi-bank environments allowing operators to key and balance transactions. • OS - Windows • Server Dependencies • NodeJS • Software Dependencies • Chrome Browser

TraxIT	• Architecture: ASP .NET web application.
	• Application Description: Application used to order equipment from the Benchmark warehouse.
	• OS – Windows
	• Server Dependencies
	  ○ SQL Server
	  ○ IIS
	• Software Dependencies
	  ○ Browser

autoMICR	• Architecture: Web-based application written in JavaScript/HTML. • Application Description: autoMICR is designed as a Blackbox solution designed to process a financial institution's X9.37 files for data perfection. The target markets are banks/financial institutions.

Application Name	Software Details

	• OS – Windows
	• Server Dependencies
	  ○ NodeJS
	• Software Dependencies
	  ○ Browser

QDS Capture	• Architecture: .NET thick client application.
	• Application Description: Application designed to interface with check handling peripherals, specifically the Quantum DS check scanner by Digital Check. Checks are scanned and processed by the application. The target markets are banks/financial institutions.
	• OS – Windows
	• Server Dependencies
	  ○ None
	• Software Dependencies
	  ○ SQL Server Express

nextStarPLUS	• Architecture: C/C++ thick client application.
	• Application Description: Application designed to interface with microfilm and microfiche conversion peripherals, specifically the Eclipse, FlexScan, FlexScan+, FlexView, and Apex scanners by nextScan. Film and fiche are scanned and processed by the application suite. The target markets are service bureaus, educational institutions, insurance agencies, and government entities.
	• OS – Windows
	• Server Dependencies
	  ○ None
	• Software Dependencies
	  ○ MySQL or SQL Server
	  ○ Apache HTTPD
	  ○ PHP

PerfectView	• Architecture: .NET thick client application.
	• Application Description: Application designed to interface with microfilm and microfiche reading peripherals, specifically the ViewScan III and ViewScan 4scanners by ST Imaging. Film and fiche are scanned and processed by the application. The target markets are anyone that has a small collection of film or fiche where the images are accessed on an on-demand basis.
	• OS – Windows
	• Server Dependencies
	  ○ None
	• Software Dependencies
	  ○ None

1. Infrastructure and Databases

CashWare, Clear by Avivatech, Vault by Avivatech, autoMICR, QDS Capture, XpressCash, XpressScan, nextStarPLUS, and PerfectView as deployed during the Specified Period run within the customers' environments. Customers are responsible for updating to new versions of the system code as they are released, and securing their environment appropriately. All code is managed through the cloud hosted version of Microsoft Azure DevOps or VisualSVN.

XpressControl is managed by Avivatech who hosts it in a Google Cloud Platform (GCP) cloud environment. Avivatech is responsible for updating code and securing these. XpressScan is also managed by Avivatech who hosts the development environment in an Amazon Web Services (AWS) cloud environment.

TraxIT is a web-based application for equipment ordering that is hosted on Windows Servers on-premises in the Company's Alpharetta, GA location.

A Microsoft SQL database is used for TraxIT and CashWare in conjunction with Microsoft Internet Information Services (IIS) front-end.

TraxIT development/test ("TraxIT dev/test") and TraxIT production runs on-premises in Alpharetta on virtualized hosts running Windows Server. Physical hosts leverage virtualization capabilities for host failover, dynamic resource allocation, and auto tiering storage. All servers have redundant power, are connected to a UPS, have multiple circuits for ISP failover, and are connected to redundant switches and redundant firewalls.

CashWare development/test ("CashWare dev/test"), Clear by Avivatech development/test ("Clear by Avivatech dev/test"), Vault by Avivatech development/test ("Vault by Avivatech dev/test"), autoMICR development/test ("autoMICR dev/test"), QDS Capture development/test ("QDS Capture dev/test"), XpressCash development/test ("XpressCash dev/test"), XpressControl development/test ("XpressControl dev/test"), and XpressScan development/test ("XpressScan dev/test") source code are all managed from the cloud hosted version of Microsoft Azure DevOps.

Clear by Avivatech, Clear by Vault, autoMICR, XpressScan, XpressCash, PerfectView, and QDS Capture do not utilize a database. autoMICR, Vault by Avivatech, and XpressCash utilize NodeJS along with a webserver. XpressControl uses Google BigQuery as its database. XpressScan utilizes PHP with an IIS front-end. QDS Capture is built off .Net and is a front-end application only. Clear by Avivatech utilizes IIS with PHP built on C++/C#. Customers are instructed to secure these applications through a Secure Sockets Layer (SSL) certificate that customers purchase and manage.

nextStarPLUS and PerfectView are running from custom built PC's that drive microfilm and microfiche hardware. nextStarPLUS development/test ("nextStarPLUS dev/test") and PerfectView development/test ("PerfectView dev/test") are run out of the DC Idaho office in Meridian, ID. All nextStarPLUS and PerfectView code changes are managed from a VisualSVN (Subversion) server running on-premises in Meridian, ID.

Systems Overview	Purpose
Microsoft Azure	System Infrastructure
Microsoft SQL Server	Data warehousing
Microsoft Entra ID Domain Services	Cloud Identity Management
Google Cloud Platform	XpressControl System Infrastructure
Google BigQuery	XpressControl Serverless Data Warehousing
Google Filestore	XpressControl Managed File Storage Service
Google VPC	XpressControl Web Application Firewall
SonicWall	Web Application Firewall
Amazon Web Services EC2	XpressScan System Infrastructure for Development Environment
On-Premise Windows Servers	TraxIT System Infrastructure
Company Owned Endpoint Devices (Laptops)	Endpoints Devices

2. Supporting Software Tools

The following supporting software tools are used to build and support the Software Services:

Supporting Software Tools	Purpose
Microsoft SharePoint	Electronic Document Management System
Microsoft Sentinel	SIEM Tool
Microsoft Defender for Endpoint	Endpoint protection
Microsoft Azure DevOps	Version Control Software
Microsoft SQL Management Studio	Database administration tool
Microsoft Intune	Mobile Device Management
Avigilon	Physical Identity Management
Xcitium	Ticket management
VisualSVN	Version Control Software
Commvault	Backup tool
OpenVPN	Virtual Private Network
Microsoft Sentinel	SIEM Tool

D. Principal Service Commitments and System Requirements

The Company makes service commitments to user entities consistent with the laws and regulations that govern the provision of those services and the operational and compliance requirements that the Company has established for the services.

Security, availability, and confidentiality commitments to user entities are documented in the terms of the license and/or applicable service agreement and communicated in other customer documents, as well as in the description of the service offerings provided online and software documentation. Security, availability, and confidentiality commitments are mostly standardized and include, but are not limited to, the following:

- The use of security principles that are designed to permit system users to access the information needed based on their role in the system while restricting them from accessing information not needed for their role;
- The use of encryption technologies to protect data in transit and at rest;
- The use of reasonable precautions to protect the security and confidentiality of the information that is collected; and
- The use of availability principles that are designed to help ensure availability of the systems supporting the system.

The Company establishes operational requirements that support the achievement of security, availability, and confidentiality commitments and other system requirements and compliance with relevant laws and regulations. Such requirements are communicated in the Company's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected.

E. Subservice Organizations

The Company utilizes a subservice organization to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Google Cloud Platform (GCP)	The Company uses Google Cloud Platform (GCP) for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The Company also uses Google Filestore and Google BigQuery as a Platform-as-a-Service. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure and software such as physical servers and physical access to backups and facilities; • Controls around the change management processes for the software and infrastructure supporting the platform; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components for Google FileStore and Google BigQuery such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over the prevention, detection, and follow up upon the introduction of malicious software; • Controls around Google FileStore and Google BigQuery redundancy, including controls over data replication and backups; • Controls over Google FileStore and Google BigQuery including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls over managing patching for the software and infrastructure supporting the platform; • Controls over the encryption of transmitted and stored data within the platform including Google FileStore and Google BigQuery; and	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over the change management processes for the Google Infrastructure-as-a-Service Platform and the Platform-as-a-Service (Google FileStore and Google BigQuery) platform components as applicable. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary • Data restore testing is performed on at least an annual basis to verify the integrity of the backup data. • The Company's production environment is configured to continuously monitor for uptime, latency, utilization, and active services, and that IT personnel were automatically notified in the event of an incident.	
Microsoft Azure (Azure)	The Company uses Microsoft Azure (Azure) for its Software-as-a-Service Entra ID Domain Services (Azure Entra ID DS). The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure supporting the Azure Entra ID DS environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure and software such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the software and infrastructure supporting the Azure Entra ID DS environment; • Controls over incident monitoring, response, and follow up; • Controls over the prevention, detection, and follow up upon the introduction of malicious software; • Controls over the monitoring of the Azure Entra ID DS components including backups, anti-virus, and incidents related to security and availability including responding to items identified; • Controls over the encryption of transmitted and stored data within the Azure Entra ID DS environment; and • Controls over managing patching for the software and infrastructure supporting the Azure Entra ID DS environment. In addition, the Company has identified the following control activity to help monitor the subservice organization:	CC 6.1* CC 6.2* CC 6.3* CC 6.4* CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary • Data restore testing is performed on at least an annual basis to verify the integrity of the backup data. • The Company's production environment is configured to continuously monitor for uptime, latency, utilization, and active services, and that IT personnel were automatically notified in the event of an incident.	
Meridian IT, Inc. (Meridian)	The Company uses Meridian IT, Inc. (Meridian) for its backup monitoring services. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls around the monitoring of the backups for the in-scope applications and related databases, including alerting and tracking of backup failures. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary.	CC 5.2* CC 6.4* CC 6.8* CC 7.5* CC 8.1* CC 9.1*
Amazon Web Services (AWS)	The Company uses Amazon Web Services (AWS) Elastic Compute Cloud (Amazon EC2) services for its third-party hosting of servers and equipment in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as network devices, routers, and servers. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression;	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; • Controls over incident monitoring, response, and follow up; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform; and • Controls over the configuration settings within the AWS EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the System and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary	CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.*

F. User Entity Responsibilities

Each user entity must evaluate its own system of internal controls for effective risk management and compliance. The internal controls described in this report occur at and are managed by the Company and only cover a portion of a comprehensive internal control structure relevant to a user entity. Each user entity must address the various aspects of internal control that may be unique to its particular organization. This section highlights those portions of the internal control structure that user entities have responsibility to develop and maintain but should not affect the ability of the Company to achieve its service commitments and system requirements.

Related Control Area	User Entity Responsibilities
Monitoring & Communication	• Customers are responsible for security configuration settings, monitoring configuration settings, and related security of the environments used to host the CashWare, XpressScan, XpressCash, XpressControl, autoMICR, QDS Capture, Clear by Avivatech, Vault by Avivatech, nextStarPLUS, and PerfectView applications. • Customers are responsible for monitoring AutoMICR application's dashboard for items flagged as "suspect" for investigation and resolution.

Related Control Area	User Entity Responsibilities
Access	• Customers are responsible for the access provisioning and de-provisioning for their environments to ensure that the User Entities' users' access is appropriate. • Customers are responsible for performing periodic user access reviews over applicable applications and systems to ensure that its users' access is restricted and limited to appropriate personnel based on job function.
Policies & Procedures	• Customers are responsible for obtaining and securing the CashWare, XpressScan, XpressCash, XpressControl, autoMICR, QDS Capture, Clear by Avivatech, Vault by Avivatech, nextStarPLUS, and PerfectView applications with Secure Sockets Layer (SSL) certificates.
Change Management	• Customers are responsible for updating to new versions of the system code as they are released for CashWare, Clear by Avivatech, Vault by Avivatech, autoMICR, QDS Capture, XpressCash, XpressScan, nextStarPLUS, and PerfectView applications.


Aprio