Proprietary & Confidential

System Description of Vista

SOC 3
Relevant to Security

SEPTEMBER 1, 2019 TO AUGUST 31, 2020

Moss Adams LLP
805 SW Broadway, Suite 1200
Portland, OR 97205
(503) 242-1447

Table of Contents

I. Independent Service Auditor's Report

MOSSADAMS

Viewpoint
1515 SE Water Avenue, Suite 300
Portland, OR 97214

To the Management of Viewpoint:

Scope

We have examined Viewpoint, Inc. and its subsidiaries' (collectively, "Viewpoint") accompanying assertion in Section II titled "Viewpoint's Assertion" (assertion) that the controls within Viewpoint's Vista (system) were effective throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that Viewpoint'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*).

Viewpoint uses subservice organization Otava and Microsoft Azure for hosting and delivering Vista. Our examination did not include the services provided by the subservice organizations

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls contemplated in the design of Viewpoint's controls are suitably designed and operating effectively, along with related controls at Viewpoint. We have not evaluated the suitability of design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve Viewpoint'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 Viewpoint's service commitments and system requirements based the applicable trust services criteria

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

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Viewpoint's Vista were effective throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that Viewpoint's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Moss Adams LLP

Portland, Oregon
November 2, 2020

II. Viewpoint’s Assertion

VIEWPOINT®
A TRIMBLE COMPANY

We are responsible for designing, implementing, operating, and maintaining effective controls within Viewpoint’s Vista (system) throughout the period September 1, 2019 to August 31, 2020 to provide reasonable assurance that Viewpoint’s service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in Section III entitled “Viewpoint’s Description of the Boundaries of Vista” and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that Viewpoint’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)*. Viewpoint’s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section III entitled “Viewpoint’s Description of the Boundaries of Vista”.

Viewpoint uses subservice organization Otava and Microsoft Azure for hosting and delivering Vista. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Viewpoint, to achieve Viewpoint’s service commitments and system requirements based on the applicable trust services criteria. The description presents Viewpoint’s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Viewpoint’s controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period September 1, 2019 to August 31, 2020, to provide reasonable assurance that Viewpoint’s service commitments and system requirements were achieved based on the applicable trust services criteria.

III. Viewpoint's Description of the Boundaries of Vista

A. System Overview

1. Services Provided

Viewpoint, a wholly owned subsidiary of Trimble, Inc., has been a construction software industry leader for more than 40 years. Since opening its doors in 1976, every success the company has experienced is a direct result of operating within its core values. Today, Viewpoint articulates those values as Character, Collaboration, Commitment, Entrepreneurship, and Resilience. These values are reflected in the people, products, and services that put Viewpoint at the technological forefront of the construction software industry.

Viewpoint is a leading global provider of integrated software solutions for the construction industry, helping contractors to digitize operations and transform their businesses for increased productivity, lower risk, and higher margins. Focused on connecting critical business functions like accounting and project management with field operations, Viewpoint's highly collaborative and intuitive cloud-based solutions can be tailored to organizations of any size.

Viewpoint solutions help more than 8,000 global customers connect the office with project teams and field operations to effectively collaborate across the broad construction ecosystem, including company owners, general contractors, subcontractors, project managers, architects, engineers, and more. Viewpoint solutions are helping transform the construction industry by aligning financial and HR systems, project management tools, and mobile field solutions to minimize risk and increase efficiency.

2. Infrastructure

Vista runs either on-premise or as a cloud application. The scope of this report does not cover on-premise instances of the Vista application. As a cloud application, Vista can be accessed in the following methods:

- Vista Remote Link (VRL): Client-side software is deployed locally and is reliant on HTTPS to connect to the Vista database server in the cloud;
- Hosted Application: Vista is reliant on virtualization technology from Microsoft to deliver Vista services as a hosted application;
- Hosted Desktop: Vista is part of a virtualized desktop, utilizing technology from Microsoft, and delivered via desktop-as-a-service model; or
- Web Access: Vista data can be accessed (read/write) through HTTPS encrypted web pages via the products, Viewpoint Financial Controls, Viewpoint Field Management, and Viewpoint HR Management. This web-based access relies on Vista authentication and does not have a separate authentication method.

From September 1, 2019 to December 31, 2019, Vista was hosted by Otava. During the period of January 1, 2020 to April 30, 2020, Otava was transitioned to Microsoft Azure. As of May 31, 2020, Vista is hosted by the following subservice organizations:

Viewpoint Product	Region	Subservice Organization
Vista	North America	Microsoft Azure
	APAC	Microsoft Azure

3. Software

Vista is a fully integrated, cloud-enabled construction management system. It consists of the following areas: accounting, project management, pre-construction, document management, equipment and asset management, human resources and payroll, materials management, purchase order, service management, and reporting.

4. People

Viewpoint's organization consists of:

- Customer-facing teams (sales, marketing, support, and services), led by the Chief Operating Officer
- Internal operations teams (facilities, finance, and information technology and information systems (IT/IS)), led by the Chief Financial Officer
- Legal and Information Security, led by the General Counsel
- Human Resources, led by the Vice President of Human Resources
- Product Management, Product Strategy, and Product Marketing, led by the Chief Products and Strategy Officer
- Product Development, Cloud Operations, and Project Management, led by the Vice President of Product Development

Vista is developed, delivered, and supported as follows:

- *IT/IS:* The IT/IS team is responsible for managing and deploying Viewpoint hardware and software infrastructure and for gaining access to cloud-based systems.
- *Product Management:* Drives the vision and product strategy to ensure Vista serves our customers, markets, and business objectives.
- *Product Development:* Vista has an allocated product development and quality assurance team responsible for maintaining and enhancing Vista and related services used by customers. These teams adhere to a secure software development lifecycle.
- *Cloud Operations:* Vista is available in the cloud delivered through the Viewpoint Cloud Operations team. This team is responsible for the day-to-day operations of the cloud systems, as well as customer support escalations as it pertains to cloud access and administration. This team is not responsible for application support.

- *Information Security Officer:* This role is responsible for managing the security policy document and ensuring control processes are followed, as well as auditing and revising policies and controls on an annual basis.
- *Customer Support:* Viewpoint has a centralized product (application) support team comprised of generalists and subject matter experts. Depending on the customer issue, different team members provide support services to the customer.
- *Human Resources:* The Human Resources team ensures that all job positions are properly described, hired according to documented practices, including background checks, and onboarded with Viewpoint, including training on best practices and procedures for security.

5. Data

All data uploaded to Vista is encrypted at rest within the primary and off-site backup data centers and the encryption keys are securely held within the Azure Key Vault. Viewpoint offers encryption at rest for its Vista customers in two different levels. Storage device-level data at rest encryption is provided for all physical disks by default at no additional charge for all hosted Vista customers. SQL database file-level data at rest encryption is optional for an added fee for those customers who require this additional layer of security.

Additionally, all data uploaded to Vista is encrypted as it transfers between the cloud environment and the separate backup cloud environment.

Cloud servers are behind a firewall and on an isolated network within their respective cloud provider infrastructures. The data is in a physically secured environment.

6. Processes and Procedures

Viewpoint has formal information security policies and procedures, which are reviewed and revised as applicable on an annual basis by the Information Security Officer. These documents are available for staff review on Viewpoint's intranet site. Viewpoint employees are required to acknowledge the policies upon commencement of employment and following significant content revisions. In addition, Viewpoint leverages a secure software development lifecycle methodology that covers the entire development process, from conception through development, testing, implementation, and modification. There is also a formal change management process for both planned changes (i.e., product updates or upgrades), as well as emergency fixes necessary to resolve a customer issue. The change management process was designed to both ensure a control exists to facilitate a process for limiting interruption of service while tracking core adaptations to the environment and to provide opportunity to notify customers of upcoming planned changes.

Vista adheres to the same segregation of duties as follows:

- *Product Development:* Modifies Vista in response to one of three scenarios:
  - *Enhancement:* New features described by product management, implemented by product development, and tested by product quality assurance.
  - *Defects:* Externally identified by customers or partners or internally identified by Viewpoint employees (e.g., product quality assurance), and subsequently fixed by product development and verified by product quality assurance.

    - *Maintenance:* Ongoing work to maintain performance levels or remain current on supported third-party applications (e.g., OS, SQL, and web-browser) is performed by product development and verified by product quality assurance.
- *Cloud Operations:* The Viewpoint Cloud Operations team follows written procedures in a runbook for delivery of Vista (i.e., major versions, service packs, and hotfixes). Situation dependent changes are required from time to time (e.g., reset a cloud-access password).
- *Customer Support:* The Viewpoint Support team responds to and resolves support tickets from customers. With customer permission, the Viewpoint Customer Support team can make administrative changes to a software application.
- *Recruiting and Talent Acquisition:* Position openings are posted on the public Viewpoint website, as well as on third-party websites such as LinkedIn and Indeed.com. The Viewpoint Human Resources team uses standardized job descriptions for each role, which clearly state required skills, experience, and other relevant requirements. Prior to an employee's first day, and except where prohibited by applicable law, the Viewpoint Human Resources team conducts a background check.

B. Principal Service Commitments and System Requirements

Viewpoint provides customers with access to and use of Vista as specified on the order signed by customers. Viewpoint designs its processes and procedures to meet its objectives for the provision of Vista delivered as a hosted application. Those objectives are based on the service commitments that Viewpoint makes to customers, applicable laws and regulations, and the financial, operational, and compliance requirements that Viewpoint has established for the services. The services provided by Viewpoint are subject to the laws and regulations in the jurisdictions in which Viewpoint provides Vista.

Viewpoint provides support for Vista in accordance with its Software Assurance Terms, available at www.viewpoint.com/legal/agreements-and-terms or any similar successor website.

Viewpoint documents its security commitments to customers in its Master Software License Agreement, which is available online at www.viewpoint.com/legal/agreements-and-terms or any similar successor website.

Viewpoint documents its data protection and compliance efforts at www.viewpoint.com/security.

Additional security commitments include, but are not limited to, the following:

- Security principles within the Vista application that are designed to permit users to access the information they need based on their role, while restricting them from accessing information not needed for their role. Roles are defined by each customer and are assigned a list of associated permissions.
- Customers may choose to use native operating system inactivity lockout methods when the computer used to access Vista is not active for a period of time. This approach allows long-running Vista processes to continue without interruption (e.g., payroll processing).
- Passwords are set up by customers and required to be of minimum length and complexity. The passwords can be set to expire on a regular basis.
- Customers may optionally activate multi-factor authentication via Microsoft Azure AD.

Viewpoint, through its third-party hosting providers:

- Helps to ensure physical and digital security protections of customer data using industry standard controls;
- Employs firewalls, intrusion detection, antivirus, and other security services;
- Deploys up-to-date advanced threat protection services, which help to identify, track, and mitigate common security risks such as environment scans, adware, malware, ransomware, spyware, Trojans, phishing attempts, and other malicious activity; and
- Uses encryption technologies to protect customer data both at rest and in transit.

Viewpoint establishes internal operational requirements that support the achievement of security commitments, compliance with relevant laws and regulations, and other system requirements. Such requirements are communicated in Viewpoint's policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and customer data are protected. These include policies related to 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 in the operation and development of the Vista application used to provide the service to customers.

C. Complementary User Entity Controls

Viewpoint's Vista was designed under the assumption that certain controls would be implemented by customers to which Viewpoint provides Vista. In these situations, the application of specific controls at these customer organizations is necessary to achieve certain control objectives included in this report.

This section describes additional controls that should be in operation at the customer organizations to complement the controls at Viewpoint. User auditors should consider whether the following controls have been placed in operation by the customers.

Each customer must evaluate its own internal control structure to determine if the identified customer controls are in place. Users are responsible for:

	Complementary User Entity Controls
1	Entering into and complying with their contraction obligations with Viewpoint.
2	Administering their own access control systems within their infrastructure.
3	Properly maintaining and notifying Viewpoint of changes or deletions to the administrative or technical contacts list.
4	Notifying Viewpoint of changes to specific contact information, such as phone numbers, emails address, fax, and/or mail addresses.
5	Creating infrastructure passwords that meet industry standard best practices for password complexity and maintain policies that support routine changes of the passwords.

Complementary User Entity Controls	
6	Implementing security, policies, and procedures that help protect their systems from unauthorized or unintentional use, modification, addition, or deletions and limit threats from connections from other networks.
7	Ensuring that the ability of customers’ employees and other authorized users to access Vista is commensurate with the responsibility assigned to those employees or users leveraging the principle of least privilege.
8	Ensuring that the customer network used to access the Viewpoint managed network is architected, engineered, and built to acceptable security standards so that the customer’s network access into the Viewpoint-managed network meets the customer’s levels of security assurance.
9	Reviewing, approving, and authorizing Viewpoint to implement recommended solutions to resolve problems escalated by the customer (if required).
10	Assuming responsibility for any loss or damage resulting from non-tested or inadequately tested customizations or integrations applied to Vista.

MOSSADAMS