ALTUS GROUP U.S., INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

ALTUS PERFORMANCE PLATFORM SYSTEM

FOR THE PERIOD OF AUGUST 1, 2023, TO JULY 31, 2024

Attestation and Compliance Services

INDEPENDENT SERVICE AUDITOR'S REPORT

To Altus Group U.S., Inc.:

Scope

We have examined Altus Group U.S., Inc.'s ("Altus Group") accompanying assertion titled "Assertion of Altus Group U.S., Inc. Service Organization Management" ("assertion") that the controls within Altus Group's Altus Performance Platform system ("system") were effective throughout the period August 1, 2023, to July 31, 2024, to provide reasonable assurance that Altus Group's service commitments and system requirements were achieved based on the trust services criteria relevant to security, and availability (applicable trust services criteria) set forth in TSP section 100, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

Altus Group uses various subservice organizations for cloud hosting and managed application firewall services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Altus Group, to achieve Altus Group's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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

Altus Group 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 Altus Group's service commitments and system requirements were achieved. Altus Group has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Altus Group 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 systems 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 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 Altus Group'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 Altus Group'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.

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 Altus Group'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 Altus Group's Altus Performance Platform system were effective throughout the period August 1, 2023, through July 31, 2024, to provide reasonable assurance that Altus Group's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Schellman & Company, LLC

Columbus, Ohio
December 2, 2024

ASSERTION OF ALTUS GROUP SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Altus Group U.S., Inc.'s ("Altus Group") Altus Performance Platform system ("system") throughout the period August 1, 2023, to July 31, 2024, to provide reasonable assurance that Altus Group's service commitments and system requirements relevant to security, and availability were achieved. Our description of the boundaries of the system is presented below 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 August 1, 2023, to July 31, 2024, to provide reasonable assurance that Altus Group's service commitments and system requirements were achieved based on the trust services criteria relevant to security, and availability (applicable trust services criteria) set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*. Altus Group's objectives for the system in applying the applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 August 1, 2023, to July 31, 2024, to provide reasonable assurance that Altus Group's service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE ALTUS PERFORMANCE PLATFORM SYSTEM

Company Background

Altus Group U.S. Inc. ("Altus Group") is a provider of independent advisory services, software, and data solutions to the global commercial real estate industry. Altus Group's businesses and Altus Analytics services reflect decades of experience, and technology-enabled capabilities. Altus Group's solutions empower clients to analyze, gain market insight and recognize value on their real estate investments. Headquartered in Canada, Altus Group has approximately 2,800 employees around the world, with operations in North America, Europe, and Asia Pacific.

Description of Services Provided

The Altus Performance Platform (APP) is the next generation tech stack delivering intelligence-as-a-service to clients. It is a new, cloud-native platform to unite the technology, analytics, and expertise together; this will help enable new integrations, data, analytics, and client applications at scale and with quality, security, and data management practices. The objective of APP is to deliver different offering solutions allowing customers to consistently improve their performance while managing their risks. These clients include both small and mid-sized business (SMB) or enterprise clients that have adopted an information technology (IT) outsourcing strategy.

APP offers are made up of products and services to include the following capabilities.

- Reduce Total Cost of Ownership (TCO) by providing a zero-infrastructure offering.
- Provide a competitive alternative solution delivery option.
- Provide scalable licensing options to align with client business needs.
- Deliver Argus solutions to users with zero server footprint for the client.
- Offer consumption-based subscriptions for different offer solutions.

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Principal Service Commitments and System Requirements

Altus Group designs its processes and procedures related to the APP environment to meet its objectives for its APP services. Those objectives are based on the service commitments that Altus Group makes to user entities, the laws and regulations that govern the provision of the APP services, and the financial, operational, and compliance requirements that Altus Group has established for the services. The APP services of Altus Group are subject to the relevant regulatory and industry information and data security requirements in which Altus Group operates.

Security and availability commitments to user entities are documented and communicated in the software subscription agreement and other customer agreements. The principal security and availability commitments are standardized and include the following:

- The use of logical access controls to safeguard the receipt, storage, and internal transfer of client data within the system boundaries.
- The development, testing, and maintenance of business continuity plans for critical functions.
- Implement change management process and procedures to maintain health and availability of systems.

- The service offerings will be available to customers with 99% uptime, not including scheduled or emergency maintenance.
- Altus Group will keep customer data confidential and only disclose confidential data to authorized parties to the minimum extent necessary.
- Ability to recover and restore customer data.

Altus Group has also established system requirements that support the achievement of the principal service commitments. These requirements include the following:

- Logical access policies are in place to guide Altus Group personnel in the provisioning of access to the in-scope systems on a need-to-know basis, performing periodic access reviews, credential management, and use of multifactor authentication.
- Change management policies and procedures are in place to guide personnel in the request, documentation, testing, and approval of changes. Change management policies and procedures are documented to outline the separation of duties in change management, ensuring that authorization, development, testing, and implementation of are segmented functions within the process.
- A security monitoring application is in place to monitor and analyze the in-scope systems for possible or actual security breaches and alert operations personnel when predefined events are detected.
- An availability monitoring application is in place to monitor the capacity and performance levels of systems supporting the services and alert operations personnel when predefined thresholds are exceeded.
- Disaster recovery plans are in place, and tested on an annual basis, to guide personnel in procedures to protect against disruptions caused by an unexpected event.

The aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Infrastructure and Software

Altus Group's APP system has outsourced infrastructure resource requirements to Amazon Web Services (AWS). Altus Group views the use of public cloud solutions like AWS as a strategic advantage allowing them to react to changing market trends and deploy services faster than traditional in-house data center management. Altus Group utilizes various AWS regions for its APP infrastructure which resides primarily on AWS platform-as-a-service (PaaS). While each AWS PaaS service may offer a different level of resiliency based on published metrics, Altus Group implements multiple availability zones for those AWS services which support this feature allowing for greater resiliency within the region.

Altus Group does not own or maintain any of the hardware located in the AWS data centers, and operates under a shared security responsibility model, where AWS is responsible for the security of the underlying cloud infrastructure (i.e., physical infrastructure, geographical regions, availability zones, edge locations, operating, managing and controlling the components from the host operating system, virtualization layer and storage) and Altus Group is responsible for securing the platform deployed in AWS (i.e., customer data, applications, identity access management, operating system and network firewall configuration, network traffic, server-side encryption).

Production infrastructure and client facing applications are logically and physically secured from internal information systems. IT personnel are responsible for maintaining the production infrastructure and information housed within the systems.

The in-scope infrastructure consists of multiple systems as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Virtual Private Network (VPN)	Encrypt remote access to the production network.	Zscaler Private Access	Zscaler
Web Application Firewalls (WAF)	WAFs using security groups allowing Altus Performance Platform the ability to configure, control, and restrict inbound network traffic into the production infrastructure within the AWS cloud environment.	Imperva WAF	Imperva
Windows Active Directory (Azure AD)	AD network domain utilized for identify access management to control access to the corporate and production networks.	Azure AD	Azure
AWS	Infrastructure and service management application.	AWS	AWS
Aurora Postgres	A cloud-native relational database engine provided by Amazon.		
Simple Storage Service (S3)	A data storage and management service provided by Amazon.		
Redshift	A fully managed cloud-based data warehouse service provided by Amazon.		

In addition, Altus Group utilizes the following systems to support APP services:

- DataDog – utilized for event monitoring metrics, infrastructure, and cloud services.
- AWS CloudTrail – utilized for logging and monitoring of AWS activities.
- AWS CloudWatch – utilized for monitoring services for AWS resources.
- AlertLogic – utilized for monitoring and protecting AWS workloads – application and infrastructure.
- Qualys – host-based scanning tool that monitors exposure, vulnerabilities, and deviations from best practices.
- ServiceNow – cloud-based platform utilized for automating IT management workflows.
- GitHub – source code management software utilized to control code versioning and security throughout the code development process.
- Jenkins – build, test, and package the application code, and then trigger the deployment process by calling deployment scripts or tools.
- Crowdstrike – cloud-based real-time threat detection utility utilized for antivirus and antimalware.

People

Personnel involved in the operation and use of the system are:

- Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Human resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).

- Offer management – responsible for driving the product line lifecycle including identifying market problems, conducting cost/benefit analysis, requirements gathering as well as time to market planning, sales enablement, etc.
- Account management – responsible for uploading a client's portfolio data into APP, ensuring the results are accurate, and providing an overview to the client.
- Customer support – responsible for level 1 (L1) support to clients' and triaging issues to level 2 (L2) support (Live Operations (LiveOps)).
- Research & development (R&D) – responsible for development and maintenance of service with a focus on key delivery areas such as solution design, service architecture, implementation, and troubleshooting. Also includes release management activities such as overseeing product/service releases with a focus on activities such as defining release objectives, managing release timelines, and identifying cross departmental dependencies.
- Quality assurance (QA) – responsible for overseeing quality of products/services. Quality starts at requirements and continues through development and testing.
- Development operations (DevOps) – responsible for automation, continuous integration and continuous development (CI/CD), infrastructure as code (IaC), and platform technical engineering.
- LiveOps - responsible for maintenance, deployment, and monitoring of the environment and security issues and incidents throughout the service delivery infrastructure.
- Accounting / finance – responsible for accounting policies, practices, and processes with a focus on accounting delivery areas such as account receivables, account payables, order management, financial reporting, and forecasts. The accounting department is also responsible for setting up managed account clients.
- Management information systems (MIS) – responsible for the design, deployment and maintenance of back-office solutions and services that support client facing products and service.

Procedures

APP clients can be assigned an Organization Administrator, Administrator, and Market Insights User role. Once a client signs a contract for APP, an initial Organization Administrator is defined and invited to the platform. They can invite additional users and assign them the necessary roles. The role assigned to a user will dictate what functionality that user can perform inside APP. Currently, stewardship functionality will be performed on behalf of a client by an account manager.

Access, Authentication, and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. To access the production application environment, users must be provisioned with login credentials which may include Azure AD cloud native, Azure AD business-to-business (B2B) federated, or security assertion markup language (SAML) federated accounts. Operational personnel are responsible for assigning and maintaining access privileges to the production environment. Administrative and elevated access privileges are restricted to the LiveOps group, using unique user accounts. The Altus Azure AD tenants are configured through policy to enforce minimum password length, password expiration intervals, password complexity requirements, and password minimum history requirements. Access to application and infrastructure components are enforced with the use of two-factor authentication.

Access Requests and Access Revocation

A formal process has been established for managing user accounts and controlling access to APP resources. Operations personnel are responsible for assigning and maintaining access rights to the corporate systems based on the individual's job role and department. Access to the APP production environment is managed by LiveOps personnel.

Upon notification of an employee termination, HR personnel provide IT and Operations personnel with a termination notice via e-mail to ensure that employees do not retain system access after their termination date. IT and Operations personnel remove any corporate and/or production environment access for the terminated employee. A termination checklist is utilized to facilitate the termination process, and a copy of the termination checklist is maintained in the employee's file. The termination checklist includes, but is not limited to, the following:

- Collection of company property
- Revocation of physical access rights
- Revocation of system access rights
- Signatures of each person that performs requisite tasks

Management requires access requests to be formally documented to ensure required activities are completed. In addition, to help ensure access privileges are authorized, operations personnel complete user access review of the corporate and production environment accounts on a quarterly basis to ensure access to data was restricted. If any individual is identified to have unauthorized access, the issue is remediated immediately.

Change Management

The change management process is used to ensure that changes to the product and system are introduced in a controlled and coordinated manner. The APP system utilizes the agile software development methodology for application development. Change management policies and procedures are documented to guide personnel in performing their duties. Releases or changes deployed to production are generally for bug fixes or new system functionality. Production changes are documented and tracked in a ticketing system. Separate development, QA, and production environments are maintained. Changes that require testing are tested in the QA environment prior to implementation. Approval for releases is obtained from the change management group prior to moving the changes to production. Approved changes are performed or managed directly by authorized LiveOps personnel; developers do not have access to the production environment. Change approval board (CAB) meetings are held on a weekly basis to review and approve upcoming changes that affect the system.

Emergency or hotfix changes undergo testing prior to their release into production. Approvals may occur after the fact based on the severity of the issue being addressed.

Version Control Software

The GitHub version control software is used as a software repository and is protected with the required access controls. GitHub records the check-in and check-out of application code, and the user account associated with the activity. Changes to source code result in the creation of a new version of the application code. The version control software provides rollback capabilities in the event application code needs to be restored to a previous version. Administrative access to the version control software is restricted to authorized personnel.

Data Backup and Disaster Recovery

The backup system is utilized to provide data backups and retention for production data. The backup system is configured to perform a full backup of production data on a daily basis. The backup system is monitored to ensure the status of these backup jobs is tracked and notifications of any issues are distributed to relevant support staff for remediation.

Disaster recovery procedures are developed and documented based on a formal risk assessment to identify threats to availability of the APP system. The recovery procedures are tested on at least an annual basis. Additionally, backup data restoration testing is performed by the information technology personnel at least annually, to ensure backup media is available.

Incident Response

Documented incident response policies and procedures are in place to guide personnel in the handling and reporting of security incidents. Internal and external users have the ability to contact customer support personnel via phone during business hours or submit an e-mail on a 24 hour a day basis in order to report system failures, incidents, concerns, and other complaints. An automated ticketing system is utilized to document security violations, responses, and resolution. Management meetings are held multiple times a week to discuss incidents

and corrective measures to ensure that incidents are resolved. Identified security vulnerabilities are triaged by operations personnel and monitored through resolution.

System Monitoring

The LiveOps team is responsible for assembling, operating, securing, and monitoring the performance of infrastructure resources, including the infrastructure, dependent services, and logical configurations of the production environment. Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization and alert the LiveOps team upon detection of unusual system activity or service requests. Enterprise monitoring applications are configured to monitor the in-scope systems capacity levels and alert IT personnel when predefined thresholds have been exceeded.

The Altus LiveOps team meets multiple times a week to discuss matters pertinent to the APP operations.

Standardized blueprint modules, infrastructure as code templates, and Jenkins pipelines are used for the build, configurations, and deployment of production infrastructure and virtual devices. These blueprints and templates help ensure consistent configurations for production environments.

Data

Browser-based access and confidential data transmissions are encrypted though the use of transport layer security protocol (TLS) (TLS1.2) to protect information transmitted. Production databases are encrypted at-rest utilizing AWS key management service (KMS).

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

Classification	Data Description	Data Reporting
Confidential	Client Portfolio data is processed by APP. Client portfolio data is stored in multi-tenant data stores (S3, relational database service (RDS), Redshift). Client Portfolio data is isolated according to the Client's Organization ID, which is assigned upon the client's purchase of APP. Client Portfolio data is presented in the Portfolio Analysis screens in APP's frontend. This data is filtered by the Client's Organization ID as well as the Client user's data permissions. Client Portfolio data can be output as a comma-separated values (csv) file by a Client's users that have the correct role and data permissions.	Client Portfolio data can be output as a csv file by end users with the correct role and data permissions.

Classification	Data Description	Data Reporting
Confidential / Personal Identifiable Information (PII)	Client user data is collected by APP, including first name, last name, e-mail address, mobile phone number (optional) in order to provision end-user access to the application. This data is stored in backend data stores as well as in AWS CloudWatch logs and Datadog logs.	The sales team will capture user information (first name, last name, e-mail address, and mobile phone [optional]) to provision the Client's Initial Organization Admin. Client user information (first name, last name, e-mail address) is accessible by a Client Organization's Org Admins and Admins via the client facing web application. Client user information (first name, last name, e-mail address, and mobile phone [optional]) is accessible by LiveOps staff as part of the day-to-day management of the system.
Confidential	Client user telemetry data (APP Org ID, User ID, and their activity within the application) is captured in Segment.io. Segment.io sends user telemetry data to APP data stores.	Client user telemetry data is accessible in Segment.io and APP data stores by LiveOps as part of day-to-day management of the system.

Subservice Organizations

The cloud hosting and managed web application firewall services provided by AWS and Imperva WAF were not included within the scope of this examination. The following table presents the applicable Trust Services criteria that are intended to be met by controls at AWS and Imperva WAF, alone or in combination with controls at Altus Group, and the types of controls expected to be implemented at AWS and Imperva WAF to meet those criteria.

Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
AWS and Imperva WAF are responsible for implementing controls to manage logical access to the underlying network, virtualization management software for its cloud hosting services where production systems reside.	CC6.1 – CC6.3 CC6.5 - CC6.6
AWS is responsible for ensuring the following: • Access to the facility hosting the production systems is restricted to personnel or visitors authorized by the tenant and reviewed periodically by management for appropriateness • Access to the facility hosting production systems is not granted to personnel or visitors unless authorized by the tenant • Access to the facility hosting the production systems is removed/disabled upon tenant notification • Access to the facility is controlled via a keycard system or other preventative access control systems • Access to the entrances and sensitive areas is monitored and/or recorded by security cameras	CC6.4
AWS is responsible for ensuring that decommissioned hardware is inventoried, stored in a secure location, and destroyed and/or wiped in accordance with established requirements.	CC6.5
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	

Control Activities Expected to be Implemented by Subservice Organizations	Applicable Trust Services Criteria
AWS is responsible for implementing controls to restrict and protect information during transmission, movement, and removal from the underlying storage devices for its cloud hosting services.	CC6.7
AWS is responsible for ensuring controls are implemented to prevent or detect and act upon the introduction of unauthorized or malicious software on the underlying network and virtualization management software and infrastructure for its cloud hosting services where production systems reside.	CC6.8
AWS and Imperva are responsible for monitoring any configuration changes of the logical access controls system for the underlying network, virtualization management, and storage devices where the production systems reside.	CC7.1 – CC7.2
AWS is responsible for monitoring physical access to facilities housing the in-scope systems to authorized personnel.	CC7.2
AWS is responsible for ensuring the data center facility is equipped with environmental security safeguards and utilizing an environmental monitoring application to monitor for environmental events.	A1.2

Complementary Controls at User Entities

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, and availability categories are applicable to the Altus Performance Platform system.