ALTUS GROUP U.S., INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

ARGUS CLOUD PLATFORM SYSTEM

FOR THE PERIOD OF NOVEMBER 1, 2022, TO OCTOBER 31, 2023

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 ARGUS Cloud Platform system ("system") were effective throughout the period November 1, 2022, to October 31, 2023, 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 a subservice organization for cloud hosting 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 organization. Our examination did not include the services provided by the subservice organization, 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.

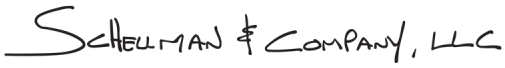
Inherent Limitations

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 ARGUS Cloud Platform system were effective throughout the period November 1, 2022, through October 31, 2023, 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.



Dallas, Texas
January 25, 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") ARGUS Cloud Platform system ("system") throughout the period November 1, 2022, to October 31, 2023, 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 November 1, 2022, to October 31, 2023, 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 November 1, 2022, to October 31, 2023, 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 ARGUS CLOUD PLATFORM SYSTEM

Company Background

Altus Group Limited provides independent advisory services, software, and data solutions to the global commercial real estate industry. Altus Group's businesses and Altus Analytics and services reflect decades of experience and technology-enabled capabilities. Altus Group's solutions empower clients to analyze, gain market insight and recognize the value in their real estate investments. Altus Group has approximately 2,800 employees worldwide, headquartered in Canada, with operations in North America, Europe, and Asia Pacific.

Description of Services Provided

The ARGUS Cloud Platform (ARGUS Cloud) aims to deliver ARGUS solutions via a hosted, subscription-priced offering to users to address zero-infrastructure requirements. These clients include small and midsized businesses (SMB) or enterprise clients that have adopted an information technology (IT) outsourcing strategy. The services address the following:

- 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 that are compatible with multiple operating systems.

ARGUS Cloud will meet the following solution from a product and process standpoint:

- Deliver ARGUS solutions to users with zero server footprint for the client.
- Offer annual, and multi-year subscriptions for ARGUS applications.

The ARGUS Cloud platform includes the following applications:

- ARGUS Enterprise - an asset and portfolio management software that helps manage property valuations, investments, portfolios, and budgeting. Key features of the enterprise application include detailing cash flow, valuation reporting, budgeting, forecasting, and transactional analysis through a cloud-hosted environment.
- ARGUS Service APIs - ARGUS Service API (The ARGUS API) opens the ARGUS Enterprise ecosystem, allowing users to have additional freedom in how they capture and use ARGUS data and the ARGUS calculation engine by providing APIs to connect industry applications and build custom tools easily.
- ARGUS Developer – an application for end-to-end management of real estate development projects. Detailed cash flow, budget, forecast and finance structures with waterfall returns, planned timescales and project phases. Run sensitivity calculations for risk analysis within the cloud-hosted environment.
- ARGUS Voyanta – a data aggregation, validation, and reporting application for users to view real estate portfolios. Enables users to consolidate data from internal and external systems, validate incoming data through a series of technical and business rules, and view entire portfolios in one consolidated dashboard.
- ARGUS Taliance – a real estate fund and alternative investment management software that enables clients to manage the performance of their real estate fund and real estate investment trusts (REITs). Customers can model complex investment structures, run scenario testing to assess the impact of market or ownership changes, calculate distribution waterfalls and create detailed reporting to stakeholders and investors.
- ARGUS Cloud Warehouse – integrates ARGUS Enterprise and ARGUS Taliance data directly into business intelligence tools and existing data warehouses. Customers can create a custom results dashboard, connect lease-level results to the investment performance or contextualize non-ARGUS data with ARGUS results. ARGUS Cloud Warehouse supplies a reporting-optimized data warehouse and data model to support customer reporting requirements.

- ARGUS Connector – provides a plug-and-play integration that enables data transfers between major industry applications and ARGUS Enterprise. This feature allows connections to property management software applications to ARGUS Enterprise on the cloud to automate the one-way data flow transfer of lease and property data directly into customer ARGUS models.

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 ARGUS Cloud system to meet its objectives for its ARGUS Cloud services. Those objectives are based on the service commitments Altus Group makes to user entities, the laws and regulations governing the provision of the ARGUS Cloud services, and the financial, operational, and compliance requirements that Altus Group has established for the services. The ARGUS Cloud 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 includes the following:

- The use of logical access controls to safeguard the receipt, storage, and internal transfer of client data within the system boundaries.
- Altus Group will use commercially reasonable efforts to make the service available 24 hours a day, seven (7) days a week, except for planned downtime.
- Altus Group will provide electronic notice for other planned downtime outside of regular daily maintenance window.
- The maintenance of the information security program including ARGUS Cloud infrastructure, technical controls, processes, policies, and certifications.
- Altus Group will keep customer data confidential and only disclose confidential data to authorized parties to the minimum extent necessary.
- Altus Group will maintain the required technical and organizational physical controls to protect customer data entrusted to Altus Group.

ARGUS Cloud 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 ARGUS Cloud personnel in the provisioning access to the in-scope systems on a need-to-know basis, performing periodic access reviews, credential management, and use of multi-factor authentication.
- System change management procedures to support the requisite, authorization, documentation, testing, and approval of system changes.
- 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.
- Deployment of application servers in auto-scaling groups across availability zones in Amazon Web Services (AWS).
- Encryption technologies to protect system user data both at rest and in transit.

- 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.
- 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 ARGUS Cloud has outsourced infrastructure resource requirements to 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 AWS' EU (Ireland) region with multiple availability zones within the region for redundancy and disaster recovery purposes to help ensure the availability of the platform.

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

ARGUS Cloud is built on a software stack comprised of AWS services, running on Windows and Linux operating systems with SQL / MySQL and MongoDB databases.

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

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Amazon Elastic Compute Cloud (EC2)	Virtualized infrastructure (servers/storage) to host ARGUS Cloud dedicated infrastructure.	Windows and Linux Operating Systems	AWS EU (Ireland) Region
Windows Active Directory (AD)	AD domain utilized to control access to the corporate and production networks.	Windows Server / AWS Directory Service	
Mongo Database (MongoDB)	Production database servers.	Linux Operating Systems	AWS EU (Ireland) Region
Microsoft SQL		SQL / MySQL	
Virtual Firewall Systems (security groups)	Firewalls allowing ARGUS Cloud the ability to configure, control, and restrict inbound and outbound network traffic into the production infrastructure within the AWS cloud environment.	AWS	

The following secondary infrastructure and supporting software is utilized in support of the delivery of the ARGUS Cloud:

- Citrix XenApp – virtual apps and desktop deployment solution.
- AWS GuardDuty – security monitoring and threat detection.
- Crowdstrike – cloud-based anti-virus / anti-malware solution.
- Qualys – continuous cloud-based vulnerability management scanning tool.
- AWS CloudWatch – monitoring tool used to track performance of AWS resources.
- PagerDuty – centralized incident management platform.
- Salesforce – subscription management system.
- Amazon relational database service (RDS) – fully managed cloud database service.
- Mange, Support, Protect (MSP360) – cloud backup and recovery software that supports local and cloud storage backup.
- GitHub – source code management software utilized to control code versioning and security throughout the code development process.

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.
- Product 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.
- Development – responsible for the development and maintenance of service with a focus on key delivery areas such as solution design, service architecture, implementation, and troubleshooting.
- Quality assurance (QA) – responsible for overseeing the quality of products/services. Quality starts at requirements and continues through development and testing.
- DevOps – responsible for creation of infrastructure design and automation.
- LiveOps - responsible for maintenance, deployment and monitoring of the environment and security issues and incidents throughout the service delivery infrastructure.
- Release management – responsible for overseeing product/service releases with a focus on activities such as defining release objectives, managing release timelines, and identifying cross departmental dependencies.
- 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 services.

Procedures

ARGUS Cloud clients can be classified as Managed Account Clients whereby clients are set up by the sales operations department. Furthermore, ARGUS Cloud users can be classified into two types: Standard User and

ARGUS Cloud Client Administrator. Standard Managed Account clients interact with the system to access the ARGUS applications hosted by the service via the ARGUS Cloud portal. Below is the standard flow:

- Access the ARGUS Cloud website.
- Enter user credentials to access the ARGUS Cloud account.
- After successful authentication, the user will be directed to the "My Applications" page.
- Users can click "Launch" to start using the application hosted by the service.
- ARGUS Cloud Citrix users will download an independent computing architecture (ICA) application on user's desktop that can be opened using the Citrix Receiver installed on user's desktop. Acquire application is web based and no download is required.
- Users can now access the ARGUS application(s) hosted by ARGUS Cloud from the user's desktop.
- Users will be able to perform actions on the ARGUS application(s) based on their permissions within the applications.

Additionally, ARGUS Cloud users can install a remote client on their machine to access ARGUS Enterprise (AE) instead of through a Citrix Client. A remote client user requires authentication to access ARGUS Enterprise with the same username and password as would be used for Citrix client.

ARGUS Cloud users can download a Microsoft (MS) Excel add-on that provides an integration between Excel and their AE instance on the ARGUS Cloud environment. Users can install the Excel add-on to their desktop and connect to their ARGUS Cloud AE instance via the plugin to retrieve or upload information to and from AE. Below is the standard flow:

- Access the ARGUS Cloud website.
- Enter user credentials to access the ARGUS Cloud account.
- After successful authentication, the user will be directed to the "My Applications" page.
- If user has access to the Excel add-on functionality, they will be able to download the installer from the page.
- Users can install the Excel add-on on the user's desktop (MS Excel is a prerequisite).
- Users can open Excel, select the "ARGUS AE" from the Excel ribbon.
- User can select "Connect to AE" tab to establish connection to their ARGUS Cloud AE instance.
- Users will create a connection by entering their ARGUS Cloud user credentials.
- On successful authentication, user will now have access to the ARGUS Excel add-on functionality from the Excel application.
- Users will be able to perform actions using the ARGUS Excel add-on based on their permissions within the applications.

In addition to the functionality above, an ARGUS Cloud Client Administrator has the ability to do the following:

- Manage user accounts – add/edit/delete user accounts including application access assignment.
- Manage security/permissions of the ARGUS applications from within the application.

Access Authentication and Authorization

Access to system information, including confidential data, is protected by authentication and authorization mechanisms. In order to access the production environment, an account user must be provisioned with AD login credentials. LiveOps personnel are responsible for assigning and maintaining access privileges to the production environment. Administrative access privileges are restricted to the LiveOps group, using unique user accounts and two-factor authentication. The network domain and application are configured to enforce minimum password length, password expiration intervals, password complexity requirements, and password minimum history requirements.

Access Requests and Access Revocation

A formal process has been established for managing user accounts and controlling access to ARGUS Cloud's resources. Corporate IT 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 ARGUS Cloud production environment is managed by the LiveOps personnel.

Upon notification of an employee termination, human resources (HR) personnel provide IT and LiveOps operations personnel with a termination notice via e-mail to ensure that employees do not retain system access subsequent to their termination date. IT and LiveOps operations personnel promptly 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 are 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 the 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, IT and LiveOps operations personnel complete user access reviews 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. ARGUS Cloud utilizes the agile software development methodology for application development. Change management policies and procedures are documented to guide personnel in performing their duties. Change management meetings are held to discuss ongoing projects and review changes that may impact the system.

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 and production environments are maintained. Changes that require testing are tested in the test environment prior to implementation. Approval for releases is obtained from the release manager prior to moving the changes to production. Approved changes are performed or managed directly by authorized LiveOps personnel. Emergency 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. Independent code review is in place to enforce separate approval by at least one individual prior to merging code to the production branch. 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 ability to modify source code is restricted to authorized users. The version control software provides rollback capabilities in the event application code needs to be restored to a previous version.

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 configured to generate and send a daily report of backup jobs, and these e-mail notifications are reviewed and retained by Altus Group to help ensure backups are successfully performed.

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

Cloud system to reside in multiple AWS availability zones. In the event one zone is unavailable, the ARGUS Cloud system is available in other AWS availability zones.

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 on a weekly basis 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. Standardized build scripts are utilized for installation and maintenance of production servers and virtual devices. These build scripts help ensure consistent configurations for production systems. 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 LiveOps personnel when predefined thresholds have been met.

Vulnerability assessments are performed by security and compliance personnel on a regular basis to identify threats and assess their potential impact to system security. Penetration tests are performed by a third-party vendor on at least an annual basis to identify threats within the production environment. Any security vulnerabilities that are detected are documented, analyzed, and monitored through resolution. Additionally, user access permissions to the production systems and AWS security groups are reviewed by management on a quarterly basis to help ensure access is monitored for authorized users.

Data

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

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Customer data processed by the hosted application. All customer data is stored in the customer specific databases. Data outputs includes reports in Excel/portable document format (PDF), proprietary XML based format (AVUX).	Customer output/data (Excel, PDF or proprietary (AVUX) format) is available to customer via the customer application.	Confidential
Proprietary files only consumable by ARGUS Cloud are stored by ARGUS Cloud in a dedicated drive for each organization.	Files are available to customer via the customer application.	
Client (name and address) and user information (name and e-mail address).	Information is accessible by admin users via the client facing web application.	Restricted

Subservice Organization

The cloud hosting services provided by AWS 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, alone or in

combination with controls at Altus Group, and the types of controls expected to be implemented at AWS to meet those criteria.

Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where the production systems reside.	CC6.1 – CC6.3 CC6.5 - CC6.6
AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 - CC6.5
AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where production systems reside.	CC6.7
AWS is 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 environmental protection controls are in place to meet ARGUS Cloud's availability commitments and requirements.	A1.2
AWS is responsible for managing the redundant infrastructure utilized and configured by ARGUS Cloud for recovery operations.	A1.3

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 ARGUS Cloud Platform system.