Altus Group

ALTUS GROUP

SOC 3® – SOC for Services Organizations: Trust Services Criteria for General Use Report

Report on the Controls within Altus Group's Finance Active Fairways Debt and Guarantees System Relevant to Security and Confidentiality

Throughout the period July 1, 2023, to June 30, 2024

Table of Contents

INDEPENDENT SERVICE AUDITOR'S REPORT 1

MANAGEMENT OF ALTUS GROUP'S STATEMENT 4

ATTACHMENT A: ALTUS GROUP'S OVERVIEW OF SERVICES AND THE FINANCE ACTIVE FAIRWAYS DEBT AND GUARANTEES SYSTEM 5

ATTACHMENT B: ALTUS GROUP'S PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 9

ATTACHMENT C: ALTUS GROUP'S COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS 10

KPMG LLP
600, de Maisonneuve Blvd. West
Suite 1500, Tour KPMG
Montreal Québec H3A 0A3
Tel 514-840-2100
Fax 514-840-2187
www.kpmg.ca

Independent Service Auditor's Report

To: Altus Group Limited

Scope

We have been engaged to report on Altus Group Limited's (Altus Group)'s accompanying statement titled "Management of Altus Group's Statement" (the Statement) that the controls within Altus Group's Finance Active Fairways Debt and Guarantees System (the System) were suitably designed and operating effectively throughout the period July 1, 2023, to June 30, 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 confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria).*

Altus Group uses the subservice organizations identified in management of Altus Group's Attachment C – Altus Group's Complementary Subservice Organization Controls (Attachment C). Management of Altus Group's Attachment C 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. Management of Altus Group's Attachment C presents the types of complementary subservice organization controls assumed in the design of Altus Group's controls. Management of Altus Group's Attachment C does not disclose the actual controls at the subservice organizations. Our engagement 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. Management of Altus Group has provided the accompanying Statement about the suitability of the design and operating effectiveness of controls within the System. Altus Group is also responsible for preparing the Statement, including the completeness, accuracy and method of presentation of the Statement; providing the services covered by the Statement; selecting, and identifying in the Statement, the applicable trust service criteria; identifying the risks that threaten the achievement of Altus Group's service commitments and system requirements; and having a reasonable basis for the Statement by performing an assessment of the suitability of the design and operating effectiveness of the controls within the System.

KPMG LLP, an Ontario limited liability partnership and member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. KPMG Canada provides services to KPMG LLP.

Our Independence and Quality Management

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality, and professional behavior.

The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements,* which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Service Auditor's Responsibilities

Our responsibility, under this engagement, is to express an opinion, based on the evidence we have obtained, on the Statement that controls within the System were suitably designed and operating effectively throughout the period to provide reasonable assurance that Altus Group's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our engagement was conducted in accordance with Canadian Standard on Assurance Engagements 3000, *Attestation Engagements Other than Audits or Reviews of Historical Financial Information*, set out in the CPA Canada Handbook – Assurance. This standard requires that we plan and perform our engagement to obtain reasonable assurance about whether the Statement 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 reasonable assurance engagement included:

- obtaining an understanding of the System and Altus Group's service commitments and system requirements;
- assessing the risks that controls were not suitably designed or did not operate effectively 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 suitably designed to provide reasonable assurance that Altus Group would achieve its service commitments and system requirements based the applicable trust services criteria if those controls operated effectively;
- testing the operating effectiveness of controls within the System to provide reasonable assurance that Altus Group's achieved its service commitments and system requirements based on the applicable trust services criteria; and
- 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 suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, the Statement that the controls within Altus Group's Finance Active Fairways Debt and Guarantees System were suitably designed and operating effectively throughout the period July 1, 2023, to June 30, 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.

KPMG LLP

Chartered Professional Accountants
Montreal, Quebec
December 16, 2024

Management of Altus Group's Statement

We are responsible for designing, implementing, operating, and maintaining effective controls within Altus Group's Finance Active Fairways Debt and Guarantees System (the System) throughout the period July 1, 2023, to June 30, 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 confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in* AICPA *Trust Services Criteria*. Our description of the boundaries of the System is presented in our Attachment A – Altus Group's Overview of Services and the Finance Active Fairways Debt and Guarantees System (Attachment A) and identifies the aspects of the System covered by the Statement.

Altus Group uses the subservice organizations identified in our Attachment C – Altus Group's Complementary Subservice Organization Controls (Attachment C). Our Attachment C 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. Our Attachment C presents the types of complementary subservice organization controls assumed in the design of Altus Group's controls.

We have performed an evaluation of the suitability of the design and operating effectiveness of the controls within the System throughout the period July 1, 2023, to June 30, 2024, to provide reasonable assurance that Altus Group's service commitments and system requirements were achieved based on the applicable trust services criteria. Altus Group'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 our Attachment B – Altus Group's Principal Service Commitments and System Requirements (Attachment B).

We confirm that the controls within the System were suitability designed and operating effectively throughout the period July 1, 2023, to June 30, 2024, to provide reasonable assurance that Altus Group's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by:
Matt Tordoff
F95BFDD0AC504FC...

Matt Tordoff
Vice President, IT Service and Operations
December 16, 2024

Attachment A: Altus Group's Overview of Services and the Finance Active Fairways Debt and Guarantees System

Company Background

Altus Group Limited (Altus Group) provides independent advisory services, software, and data solutions to the global commercial real estate industry. Altus Group's businesses, Altus Analytics and Expert 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.

Finance Active, a wholly owned subsidiary of Altus Group since 2021, develops and provides Altus Group's Finance Active Fairways Debt and Guarantees System, a cloud based financial software and financial advisory services to help clients manage their debt and guaranties. The Finance Active subsidiary was founded in 2000, headquartered in Paris and has approximately 160 employees. Originally focused on the French public sector, Finance Active next developed its activity and the Finance Active Fairways Debt and Guarantees solution to address the corporate and financial sector in the Europe which currently represents a major part of its activities.

Description of the Services Provided

The Fairways technology is a solution for corporate and financial sectors, including commercial real estate. The Finance Active Fairways Debt and Guarantees System is comprised of the following:

Finance Active Fairways Debt System

Fairways Debt system is also known as Debt Management system. For the purposes of this report, it is referred to as the Fairways Debt system.

Fairways Debt system strives to industrialize complex and resource-consuming monitoring. It is integrated into the information system and connected to several financial market data providers to collect financial data such as exchange rates. The Fairways Debt system offers the following features:

- Monitoring of debt;
- Access near-time market data;
- Evaluate and simulate strategies, costs;
- Access strategic reports;
- For Financial Institutions;
- Debt fund management;
- Loan management; and
- Supranational debt management.

The Fairways Debt system is available on two instances, on an EU instance for European clients and a North American instance for North American clients. Both are made available using the same infrastructure and from the same location as described in this report.

Finance Active Fairways Guarantees System

The Fairways Guarantees system offers the following features:

- Monitoring of guarantees;
- Access information about guarantees; and
- Report design to have a real-time view of the status of guarantees.

The Finance Active Fairways Guarantees System is available on a single EU instance for European clients.

Components of the System Used to Provide the Services

Infrastructure

The Finance Active Fairways system is hosted in AWS cloud and an Equinix data center, who are expected to have in place appropriate physical and logical access controls to protect the system from unauthorized access. Logical access to the System by Altus employees is controlled by Okta identity management service.

The system's infrastructure is protected by a DMZ, in which load balancing solutions are leveraged to balance load internally and forward traffic to the requested services hosted on containers and virtual machines. Databases and files are replicated.

Software

The Finance Active applications are Java based.

Finance Active Fairways Debt system is made of several services which are designed around:

1. Frontend architecture

Leverages already established front-end frameworks and connects to the API Gateway using secure REST APIs.

2. Public API Gateway

Provides security, monitoring and routing functionalities. It connects to the Auth module using secure REST APIs.

3. Authentication module

The Finance Active Fairways solutions leverage a cloud provider (Auth0) specialized in authentication and designed to be integrated in applications like Finance Active's. It offers integration with customers' identity management tools, including Identity Federation.

4. Backend

Finance Active Fairways Debt backend is composed of several microservices, leveraging well-known Java components. Web-services connect to Databases and other services to store data, manage cache and queues.

The Finance Active Fairways Guarantee system has a more traditional model without microservices and leverages well-known Java components as well. Web-services connect to Databases and other services to store data, manage cache and queues.

Altus relies on the services provided by AWS, Equinix, Okta, and Auth0 to operate and secure the Altus system; in designing its controls Altus has made certain assumptions about the design and operating effectiveness of the controls at AWS, Equinix, Okta, and Auth0; at least annually Altus obtains and reviews SOC 2 reports from AWS, Equinix, Okta, and Auth0 to help validate Altus' assumptions about the controls in place at AWS, Equinix, Okta, and Auth0; and for further details see Appendix C.

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**
Debt and guarantee customer data processed by the hosted applications. Data is stored in a multi-tenant database. Data outputs include reports in Excel, PDF, and JSON format.	Customer output / data Excel, PDF and JSON format is available to the customer via the customer applications.	Confidential.
Client attached document stored on servers and on AWS S3.	Files are available to customers via the customer applications.	Confidential.
User Information (name, email address).	Information is accessible by authorized Admin users of Altus Group, Admin users of clients within their own organization, via the customer applications.	Confidential.

People

Altus Group has a staff of approximately 100 employees that manage the Finance Active Fairways Debt and Guarantees system, organized in the following functional areas:

- Corporate: Executives, senior operations staff, and company administrative support staff, security and risk and compliance, incident management staff, cyber operations staff (SOC team), accounting, finance, procurement, human resources. These individuals don't use the Fairways solutions.
- Operations: Staff involved in the Customer relationship. Operations are comprised of:
  - Customer Success representatives are the main contact of customers, they are responsible for responding to customers' requests;
  - Professional Services staff are involved in the onboarding process of new clients and customizing the application for the client's needs; and
  - Support team provides level 2 support (escalation from customer success team).
- Research & Development: The team in charge of designing, developing the solutions:
  - Product team is responsible of designing new features;
  - Developer Team is responsible of implementing new features; and
  - Quality team is responsible testing the quality of deliverables.
- DevOps / Enterprise Ops: Responsible for the hosting of the services, designing, building, maintaining and operating infrastructure supporting the solutions.
- IT Services / HelpDesk: The team provides technical assistance to Altus employees.

Processes and Procedures

Management has developed and communicated to employees and contractors its policies, procedures, and documentation to promote security throughout the company. These policies and procedures are reviewed annually and approved by senior management and / or CISO. These documents cover the following key security areas:

- Global information security policy, defining strategic security objectives of Altus Group
- Information system security policy:
  - Context and objectives:

    - Objectives;
    - Security requirements; and
    - Exception procedure.
  - Organization measures:
    - Data classification and data processing;
    - Security in HR process;
    - Security in the development process;
    - Security in infrastructure operations;
    - Event and incident management; and
    - Regulatory compliance.
  - Operational measures:
    - Asset management;
    - Identity and access management;
    - Administration;
    - Workstation security;
    - Anti-malware protection;
    - Vulnerability management;
    - Cryptography management;
    - Networks;
    - Audit;
    - Backups;
    - Project and development;
    - Maintenance and disposal; and
    - Physical security.
- Information system security policy annexes:
  - Data protection policy;
  - Secret management policy;
  - Mobile device policy; and
  - Remote Working policy.
- Risk management procedure
- Whistleblower policy.

Attachment B: Altus Group's Principal Service Commitments and System Requirements

Altus Group designs its processes and procedures related to the Fairways solutions to meet its objectives for its Fairways Debt and Guarantees System. Those objectives are based on the service commitments that Altus Group makes to user entities, the laws and regulations that govern the provision of cloud services, and the financial, operational, and compliance requirements that Altus Group has established for the services. Additionally, to address the global security requirement from its clients, Altus Group's commits to design, implement and operate controls supporting the provision of a confidential environment for its services and their related data.

Security and confidentiality commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. In the context of this report, security and confidentiality commitments include the following:

- Inclusion of security principles within the designs of the Fairways system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- Tenant segregation, to ensure that a user from one client cannot access data from other clients;
- Use of encryption technologies to help protect customer data both at rest and in transit;
- Identity Federation connector to enable strong authentication from clients' systems;
- Data in production will be erased no later than 3 months after the end of the client contract; and
- Data in backups will be erased no later than 10 years after the end of the client contract.

Altus Group has implemented a certified ISO 27001 Information Security Management System to help ensure the security requirements are reviewed, improved, audited, and risk based driven. Altus Group's Information Security Management System (ISMS) establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements.

Security and confidentiality requirements are communicated in Altus Group'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. These include policies around 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 Fairways system.

Attachment C: Altus Group's Complementary Subservice Organization Controls

Altus Group uses subservice organizations to provide physical data center and authentication services. The table below describes the subservice organizations, summary of services provided and the types of controls that Altus Group has assumed to be in place during its design, implementation, and evaluation of Altus Group's controls. Note that the following are only high-level descriptions of the types of controls assumed to be in place; they are not the actual controls in place at the subservice organizations.

Subservice Organization (carved out)	Expected Subservice Organization Controls	Service Provided
Equinix	Equinix is expected to maintain industry-standard security controls for its Datacenter services. Equinix is responsible for protecting the facilities of the Datacenter. Major control areas include: – Data center access limited to authorized data center technicians; – Biometric scanning for controlled data center access; – Security camera monitoring at data center locations; – 24 × 7 onsite staff provide additional protection against unauthorized entry; – Unmarked facilities to help maintain a low profile; and – Physical security audited by an independent firm.	Dedicated physical server cabinets Data center physical security Physical access control
AWS	AWS is expected to maintain industry-standard security controls for the services provided. AWS is responsible for protecting the infrastructure that runs all the services offered in the Amazon Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS. AWS Services in scope are AWS S3 – Simple Storage Services for high integrity object and data storage. Major control areas include: – Data center access limited to authorized data center technicians; – Biometric scanning for controlled data center access; – Security camera monitoring at data center locations; – 24 × 7 onsite staff provide additional protection against unauthorized entry; – Unmarked facilities to help maintain a low profile; – Physical security audited by an independent firm; – Cloud infrastructure patch & vulnerability management; – Cloud infrastructure backups and systems monitoring; – Restricted logical access; – Backup storage and retention; and – Data redundancy and high integrity.	Data and backup storage as a service Retention policy Destruction of discontinued data assets Data encryption services Logical separation of hosting environments Logical Access control Data center physical security Logging centralization Security monitoring tooling

Subservice Organization (carved out)	Expected Subservice Organization Controls	Service Provided
Auth0	Auth0 is responsible for protecting the global authentication process and its related data. Major control areas include: – Secured password storage; – Secured authentication process; and – Monitoring for suspicious activity on authentication API.	Authentication as a service Identity provider service Identity federation service
		Data encryption services
		Logging centralization Security monitoring tooling
Okta	Okta is responsible for protecting the global authentication process and its related data. Major control areas include: – Secured password storage; – Secured authentication process; and – Monitoring for suspicious authentication activities.	Identity provider services Identity federation services
		Data encryption services
		Logging centralization Security monitoring tooling