ALTUS GROUP U.S., INC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT

FOR THE

FAIRWAYS DEBT AND GUARANTEES

FOR THE PERIOD OF NOVEMBER 1, 2024, TO OCTOBER 31, 2025

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 Fairways Debt and Guarantees system ("system") were effective throughout the period November 1, 2024, to October 31, 2025, 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, 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 Fairways Debt and Guarantees system were effective throughout the period November 1, 2024, through October 31, 2025, 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 4, 2025

Altus Group

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") Fairways Debt and Guarantees system ("system") throughout the period November 1, 2024, to October 31, 2025, to provide reasonable assurance that Altus Group's service commitments and system requirements relevant to security and confidentiality 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, 2024, to October 31, 2025, 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, *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 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, 2024, to October 31, 2025, 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 Fairways Debt and Guarantees System

Company Background

Altus Group U.S., Inc. (Altus Group) 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 1,800 employees worldwide, headquartered in Canada, with operations in North America, Europe, and Asia Pacific.

Altus Group and Finance Active, a wholly owned subsidiary of Altus Group since 2021, develop and provides Altus Group's description of its Fairways Debt and Guarantees system, a cloud based financial software and financial advisory services to help clients manage their debt and guarantees. Finance Active subsidiary was founded in 2000, headquartered in Paris and has approximately 160 employees. Originally focused on the French public sector, Finance Active further developed its activity in the Fairways Debt and Guarantees system to address the corporate and financial sector in Europe.

Description of Services Provided

Since its origin in 2000, Altus Group has provided its software as web applications in a multi-tenant Software-as-a-Service (SaaS) model. Fairways Debt and Guarantees is for corporate and financial sectors, including commercial real estate.

<u>Fairways Debt</u>

Fairways Debt (also known as Debt Management) strives to industrialize complex and resource-consuming monitoring. It is integrated into the information system and connected to the market. The Fairways Debt system offers the following features:

For the corporate sector, including commercial real estate:

- Monitor of debt;
- Access near-time market data; and
- Access strategic reports.

For financial institutions:

- Debt fund management;
- Loan management; and
- Supranational debt management.

Fairways Debt system is available on two instances – one EU instance for European clients and one U.S. instance for North American clients. Both are made available using the same infrastructure and from the same location as described in this report.

<u>Fairways Guarantees</u>

Fairways Guarantees offers the following features:

- Monitoring of Guarantees;
- Access information about guarantees; and
- Design report to get a real-time view of the status of guarantees.

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 Fairways Debt and Guarantees system to meet its objectives for its Fairways Debt and Guarantees 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 cloud services, and the financial, operational, and compliance requirements that Altus Group has established for the services. Additionally, to 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), Non-Disclosure Agreements (NDAs), and other customer agreements, as well as in the description of the service offering provided online. The principal security and confidentiality commitments are standardized and include the following:

- Integration of security principles into the design of the Fairways Debt and Guarantees, users are granted access only to the information they need to perform their duties, while limiting access to data on a need-to-know basis.
- The maintenance of the information security program including Fairways Debt and Guarantees' infrastructure, technical controls, processes, policies, and certifications. The maintenance of a change management process to identify the need for changes, implement changes in a controlled manner, and prevent unauthorized changes from being made.
- A tenant segregation is configured to ensure that a user from a 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 contract.
- Data in backups will be erased no later than 10 years after the end of the contract.

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

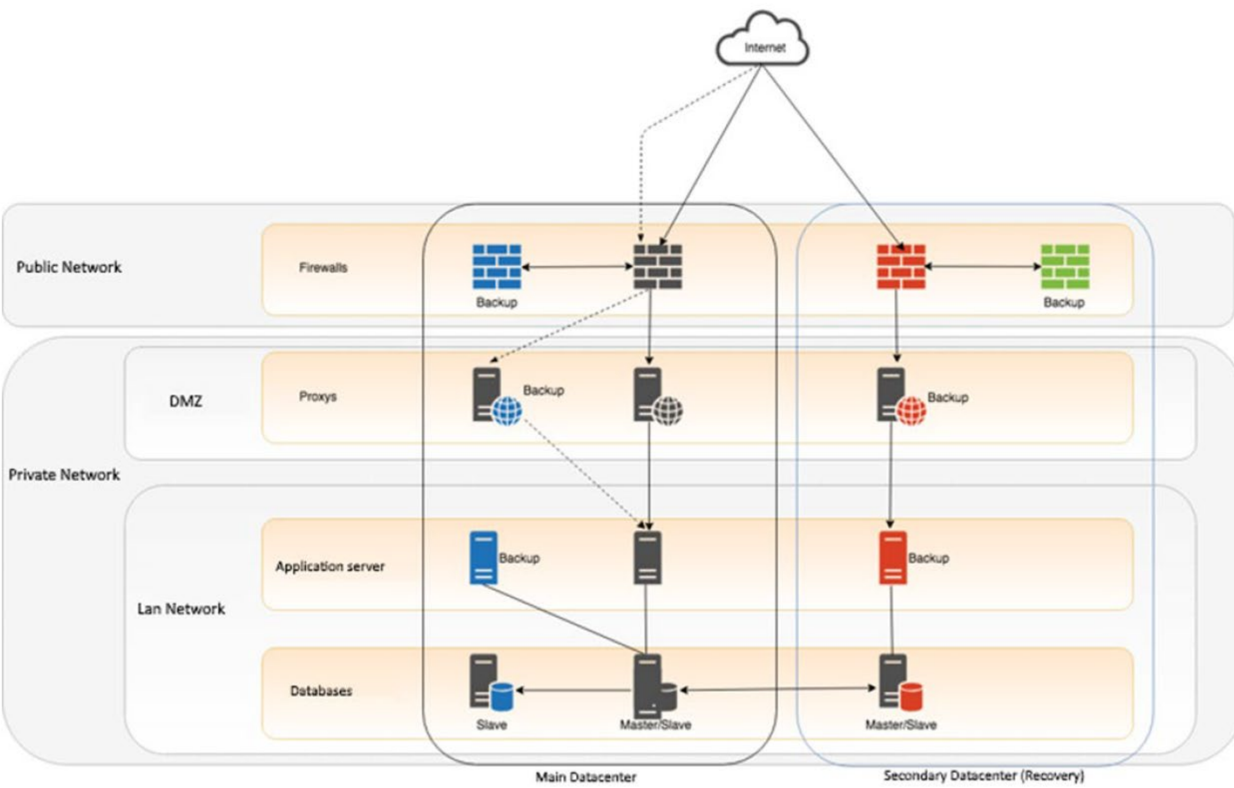
- Logical access policies are in place to guide Altus Group personnel in provisioning access to the in-scope systems on a need-to-know basis, performing periodic access reviews, credential management, and use of multifactor authentication.
- The use of firewalls to protect its network from the Internet.
- Data encryption is utilized to protect production data at rest and prevent improper alteration or destruction.
- Technical configuration implemented to limit employee access on a need-to-know basis.
- Employees are required to sign nondisclosure agreements as part of the onboarding process to ensure confidential data is only disclosed as permitted by agreements.
- 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 that outline that change management separation of duties such that authorization, development, testing, and implementation 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.

The aforementioned service commitments and requirements are those principal service commitments and requirements common to the general 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

The Fairways Debt and Guarantees system is based in two data centers located around Paris, France. The two data centers are mainly used in active-passive mode and in an active-active cluster mode for few services.

The two data centers are from Equinix, which provides power, connectivity, inter-site network, A/C, fire detection, and prevention, surveillance, and physical security. Altus Group rents several server cabinets and then hosts the servers itself. Altus Group is responsible for securing the servers (i.e., customer data, applications, identity access management, operating system and network firewall configuration, network traffic, server-side encryption).



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

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
Auth0 / Okta	Utilized for protecting the global authentication process and its related data.	Cloud-based Software-as-a-Service (SaaS)	Third-Party data centers
Chef	Configuration management and automation tool for development operations (DevOps).	Cross-platform (Linux, Windows, MacOs)	
Gitlab	Utilized to manage the software development lifecycle – planning, coding to testing, deploying, and monitoring.	Gitlab	

Primary Infrastructure			
Production System	**Business Function Description**	**Platform**	**Physical Location**
RunDeck / Simple Storage Services (S3)	Utilized as a backup system for objects and data storage.	AWS	AWS
MySQL, MongoDB, ElasticSearch	Database management systems utilized to store data and various formats.	Third party	Third-party data centers
Web Application Firewall (WAF)	Firewall and routing platform that provides network security, traffic management, and monitoring.	Imperva	
Virtual Private Network (VPN) with Multi-factor authentication (MFA)	Utilized for secure encrypted connection with MFA.	Tailscale	

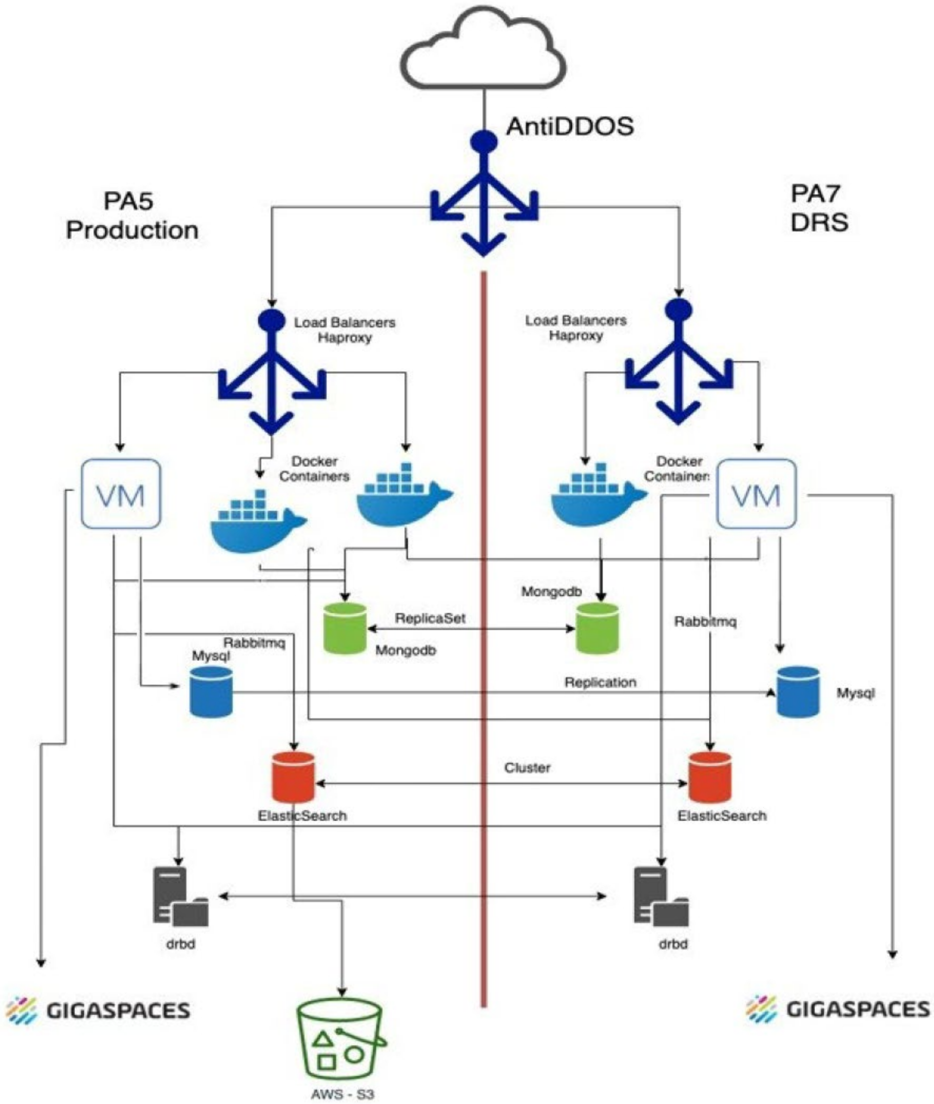
The following secondary infrastructure and supporting software is utilized in support of the delivery of Fairways Debt and Guarantees system:

- Qualys – continuous cloud-based vulnerability management scanning tool.
- CrowdStrike – utilized as a cloud-based anti-virus / anti-malware solution, host-based intrusion detection system, intrusion detection system (IDS), and intrusion prevention system (IPS).
- Centreon – IT infrastructure monitoring software designed to help monitor the health, performance, and availability of IT systems, networks, applications, and services.
- Graylog - Security incident and event management (SIEM) solution that helps detect, analyze, and respond to security threats.
- HackerOne – External web application penetration testing.
- ServiceNow – centralized incident management platform.
- Netbox – IT asset monitoring software designed to monitor physical server and virtual machine held at data centers.
- Vault – key management system (KMS) used to store secret keys to access data held within the production environment and databases.

Service Architecture

The Fairways Debt's service is exposed on the Internet through an Anti-distributed denial of Service (Anti-DDOS) cloud service.

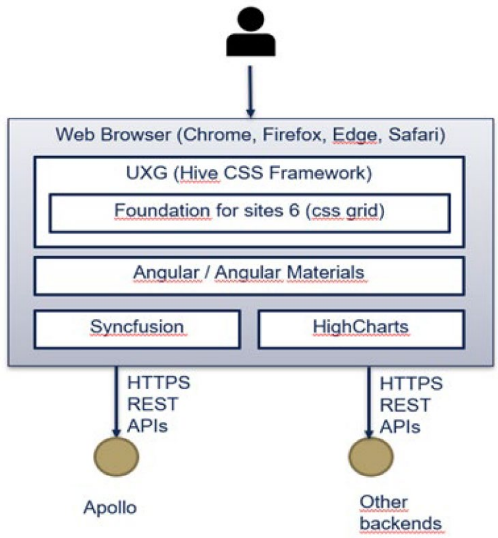
The load balancers are setup to forward the flow of traffic in the Equinix data centers on a HAProxy server in a demilitarized zone (DMZ). HAProxy will also load balance internally and forward the requested services.



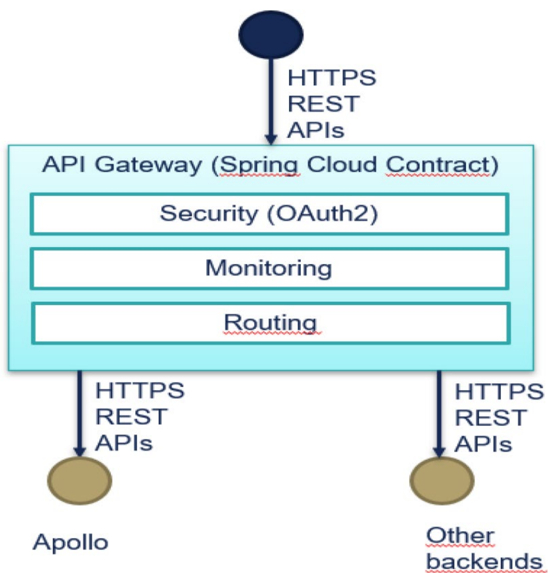
[Intentionally Blank]

The Fairways Debt is Java based and is made of several services which are designed around:

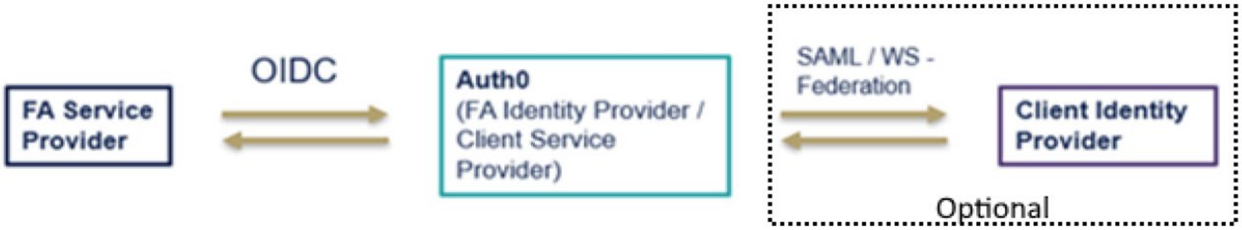
1. Front-end architecture



2. Public API gateway

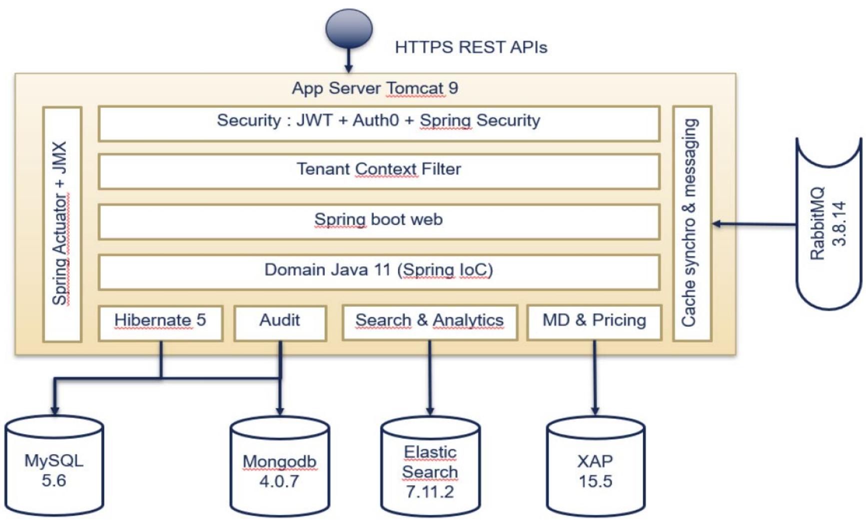


3. Authentication module
    - The Fairways Debt is protected by Auth0 authentication services. Auth0 is a cloud provider specialized in authentication and designed to be integrated with the Fairways Debt.
    - Through Auth0, the Fairways Debt system offers, by default, a standard login password authentication. To provide better integration with customers Identity and Access Management (IAM) tools and more authentication configuration capabilities, the company also offer identity federation as an option.



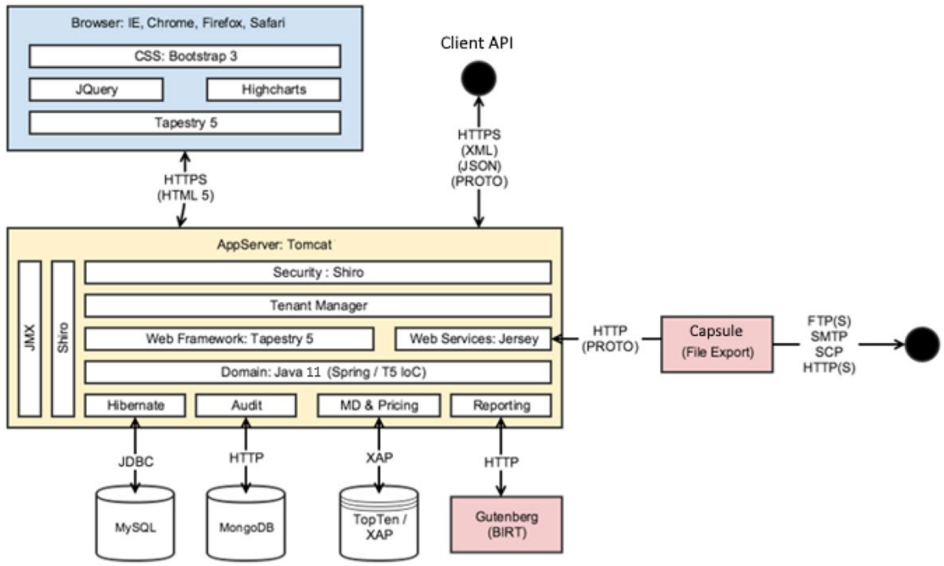
4. Backend application architecture

<u>Application V2 architecture</u>



[Intentionally Blank]

The Fairways Debt Guarantees system has a more monolithic architecture which is described below:



People

The Finance Active subsidiary has a staff of approximately 160 employees reporting to Altus Group business lines and organized them in the following functional areas:

- Corporate personnel (do not use the Fairways Debt and Guarantees):
  - Executive management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
  - Senior operations staff and company administrative support staff – responsible for managing and ensuring continuous running of business operations.
  - Security and compliance – responsible for protecting data, systems and infrastructure while ensuring company meets legal, regulatory and industry standards.
  - Human Resources (HR) – responsible for hiring, training, and performance management practices that very that employees possess the required skills and meets organization's expectations.
  - 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.
- Operations: Staff involved in the customer relationship. Operations are comprised of:
  - Customer Success representatives are main contact of customer, they answer to customers' requests, get their feedback, etc.;
  - Professional Services staff are involved in the onboarding process of new clients, customize the application for the client's needs; and
  - Support team is the main contact for a few clients and is level two support for other clients.
- Research and Development (R&D): The team in charge of designing and developing the solutions:
  - Product team is the staff in charge of designing the new feature;
  - Developer Team is the staff in charge of implementing the new feature; and
  - Quality team is the staff in charge of testing the quality of deliverables.

- DevOps / Enterprise Operations: The team in charge of the hosting of the services, designing, building, maintaining and operating infrastructure supporting the solutions.
- IT Service / Helpdesk: The team provides technical assistance to employees.

Policies and Procedures

Management has developed and communicated to employees and contractors, 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 policies and procedures cover the following key security areas:

- Global Information Security Policy -
  - Strategic security objectives of the Company.
  - the roles and responsibilities in the security function.
- Information System Security Policy -
  - Context and objectives:
    - Objectives, security requirements, and exception procedures.
  - Organization measures:
    - Data classification and data processing
    - HR process
    - Development process
    - Infrastructure Operations
    - Incident management
    - Regulatory compliance
  - Operational measures:
    - Asset management
    - IAM management
    - Administration
    - Workstation security
    - Anti-malware protection
    - Vulnerability management
    - Cryptography management
    - Networks
    - Audit
    - Backups
    - Project and development
    - Maintenance and disposal
    - Physical security

Additional policies and procedures such as data protection, secret management policy, mobile device policy, remote working policy, and risk management procedures can be found on the corporate intranet and are made available to internal employees.

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. Authorized Altus Group admin personnel are responsible for assigning and maintaining access privileges to the production environment. Administrative access privileges are restricted to the Altus Group's employees, 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 Fairways Debt and Guarantees' system 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 Fairways Debt and Guarantees system production environment is managed by the Altus Group admins.

Upon notification of an employee termination, HR personnel provide IT and Fairways Debt and Guarantees personnel with a termination notice via e-mail to ensure that employees do not retain system access subsequent to their termination date. IT and Fairways Debt and Guarantees system's admin 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 Fairways Debt and Guarantees system's admin personnel complete user access reviews of the corporate and production environment accounts on a quarterly basis to ensure access to data is restricted. If any individual is identified to have unauthorized access, the issue is remediated immediately.

Physical and Environmental Security

Equinix is responsible for the establishment and management of the Paris, France data center facilities infrastructure, physical and environmental controls, and the ongoing maintenance of said facility.

Physical access to the data centers requires a documented request form and manager approval prior to access being provisioned. Only authorized Altus Group users are allowed to access the Equinix data centers. Authorized users are escorted by Equinix personnel to the Altus Group's managed cabinets and server storage racks area only. Upon employee termination, physical access is revoked for employees within 24 hours as part of the termination process. Access to the data centers are reviewed by management on an annual basis.

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. Altus Group utilizes the agile software development methodology for application and infrastructure-as-a-code (IaaS) development. Change management policies and procedures, including the systems development life cycle (SDLC), are documented to guide personnel in performing their duties.

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 prior to moving the changes to production. Approved changes are performed or managed directly by authorized Altus Group personnel.

The Gitlab version control software is used as a software repository and is protected with the required access controls. The ability to modify source code is restricted to authorized users. The version control software provides users with the ability to restore to a previous version. Baseline configurations are retained within the configuration management tool for centralization and rollback.

Altus performs monthly review of the patching status for user endpoints and where there are identified issues, a corrective action is implemented.

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 monthly 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 Fairways Debt and Guarantees 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 builds are utilized for installation and maintenance of production servers. These builds 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 Fairways Debt and Guarantees 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 Fairways Debt and Guarantees 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 are reviewed by management on an annual basis to help ensure access is monitored for authorized users.

Data

Customer data is hosted within MySQL and MongoDB, which is stored in an encrypted format at-rest and when in-transit. The encryption configuration protocol used to secure data-in-transit is Transport Layer Security (TLS) protocol. For data-at-rest, Transparent Data Encryption (TDE) is utilized to encrypt the database files on disk using Advanced Encryption Standard (AES) algorithms.

Access to data held within the production environment and databases requires the use of a Secure Shell (SSH) key being applied. SSH keys are maintained within the Vault KMS, which can only be accessed by users with system administrator rights. Keys are rotated every 13 months in accordance with the standards established by the Change Advisory Board (CAB).

Altus Group has implemented policies and procedures to guide users in the safe handling and destruction of physical media. A third-party vendor is engaged to handle the destruction of obsolete physical media, which is performed annually.

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

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
Fairways Debt and Guarantees customer data processed by the hosted application. 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.	

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
User information (Name and e-mail)	Information is accessible by authorized Admin users of Altus Group and Admin users of clients within their own organization via the customer applications.	Confidential

Subservice Organization

The data center hosting services provided by Equinix 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 Equinix, alone or in combination with controls at Altus Group, and the types of controls expected to be implemented at Equinix to achieve Altus Group's principal service commitments and system requirements based on the applicable trust services criteria.

Ref.	Control Activities Expected to be Implemented by Subservice Organization	Applicable Trust Services Criteria
CSOC.01	Equinix is responsible for managing industry-standard security controls for its data center services. Equinix is responsible for protecting the facilities of the data center. 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 • 24x7 onsite staff provide additional protection against unauthorized entry • Unmarked facilities to help maintain a low profile • Physical security audited by an independent firm	CC6.1 CC6.4 CC8.1

Complementary User Entity Controls

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 confidentiality categories are applicable to the Fairways Debt and Guarantees system.