Options Technology Ltd.
Type 2 SOC 3
2020

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

November 1, 2019 To October 31, 2020

Table of Contents

SECTION 1

ASSERTION OF OPTIONS TECHNOLOGY LTD. MANAGEMENT

ASSERTION OF OPTIONS TECHNOLOGY LTD. MANAGEMENT

January 29, 2021

We are responsible for designing, implementing, operating, and maintaining effective controls within Options Technology Ltd.'s ('Options IT' or 'the Company') Infrastructure-as-a-Service (IaaS) - Options Platform Services System throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Options IT's service commitments and system requirements relevant to Security and Availability (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Options Technology Ltd.'s Description of Its IaaS - Options Platform Services System throughout the period November 1, 2019 to October 31, 2020" 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, 2019 to October 31, 2020, to provide reasonable assurance that Options IT'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Options IT's objectives for the system in applying 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 "Options Technology Ltd.'s Description of Its IaaS - Options Platform Services System throughout the period November 1, 2019 to October 31, 2020".

Options IT uses Cyxtera, Digital Realty Trust, Equinix, Iron Mountain, Telehouse, and Telstra to provide data center hosting services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Options IT, to achieve Options IT's service commitments and system requirements based on the applicable trust services criteria. The description presents Options IT's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Options IT's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Options IT's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Options IT's controls.

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

We assert that the controls within the system were effective throughout the period November 1, 2019 to October 31, 2020 to provide reasonable assurance that Options IT's service commitments and system requirements were achieved based on the applicable trust services criteria.

Nick Bryant
Chief Administrative Officer- Americas
Options Technology Ltd.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Options Technology Ltd.

Scope

We have examined Options IT accompanying description of IaaS - Options Platform Services System titled "Options Technology Ltd.'s Description of Its IaaS - Options Platform Services System throughout the period November 1, 2019 to October 31, 2020" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Options IT'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, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Options IT uses Cyxtera, Digital Realty Trust, Equinix, Iron Mountain, Telehouse, and Telstra to provide data center hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Options IT, to achieve Options IT's service commitments and system requirements based on the applicable trust services criteria. The description presents Options IT's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Options IT's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Options IT, to achieve Options IT's service commitments and system requirements based on the applicable trust services criteria. The description presents Options IT's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Options IT's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Options IT 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 Options IT's service commitments and system requirements were achieved. Options IT has provided the accompanying assertion titled "Assertion of Options Technology Ltd. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Options IT is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. 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, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are 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, management's assertion that the controls within Options IT's IaaS - Options Platform Services System were suitably designed and operating effectively throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that Options IT's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Options IT's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Options IT, user entities of Options IT's IaaS - Options Platform Services System during some or all of the period November 1, 2019 to October 31, 2020, business partners of Options IT subject to risks arising from interactions with the IaaS - Options Platform Services System, and those who have sufficient knowledge and understanding of the complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
January 29, 2021

SECTION 3

OPTIONS TECHNOLOGY LTD.’S DESCRIPTION OF ITS IAAS - OPTIONS PLATFORM SERVICES SYSTEM THROUGHOUT THE PERIOD NOVEMBER 1, 2019 TO OCTOBER 31, 2020

OVERVIEW OF OPERATIONS

Company Background

Founded in 1993, Options IT is a technology solutions provider to asset management firms, investment banks and financial software vendors around the world. Options IT pioneered the financial technology Infrastructure-as-a-Service (IaaS) model with the Options IT Private Financial Cloud platform now leveraged by more than 250 firms globally.

Options IT introduced the “cloud-based services” concept for financial services in 2000 through the development of a robust, scalable, comprehensive, and process-driven managed services platform. Services were expanded to the United States in 2005 and then to Asia in 2006. Today, the Company provides on-demand private cloud and 24/7 managed services to hedge funds, investment banks, and software vendors via 28 data centers globally.

Description of Services Provided

Options IT offers its customers the ability to obtain a full suite of essential technology services without the need to acquire and maintain expensive hardware, connectivity, software, or technology staff. The Options IT Private Financial Cloud delivers the scalability, strength and security of an enterprise platform with the efficiencies of a hosted solution.

Options IT services include financial application hosting and management, direct market data and execution venue connectivity, and the complete suite of desktop and communication technology essential to financial services firms. Options IT services are provided on a subscription basis. The services Options IT provides to its customers are described below:

- Managed Platform
- Managed Colocation
- Managed Applications

Principal Service Commitments and System Requirements

Options IT designs its processes and procedures related to managed services to meet its objectives for its services. Those objectives are based on the service commitments that Options IT Technology makes to user entities, the laws and regulations that govern the provision of managed services, and the financial, operational, and compliance requirements that Options IT Technology has established for the services. The managed services of Options IT Technology are subject to the privacy security laws and regulations in the jurisdictions in which Options IT Technology operates.

Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

Security principles within the fundamental designs of the services 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.

Options IT Technology establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Options IT Technology’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 services.

Components of the System

Infrastructure

Primary infrastructure used to provide Options IT's IaaS - Options IT Platform Services System includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Cisco	Data network switch	Ethernet Switch
Arista	Data network switch	Ethernet Switch
HP 3PAR	Storage Area Network	Storage
Pure	Storage Area Network	Storage
Fortinet	Firewall / VPN (virtual private network)	Firewall / VPN
HP	Enterprise Servers	Compute

Software

Primary software used to provide Options IT's IaaS - Options IT Platform Services System includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
Atlassian Jira	Cloud	Issue Tracking System
Citrix	N/A	Remote Access
VMware	VMware	Virtualization
Nagios	N/A	Monitoring
Splunk	N/A	Security Information and Event Monitoring

People

The Options IT staff provides support for the above services in each of the following functional areas:

- Executive management - provides general oversight and strategic planning of operations
- Development team - responsible for delivering a responsive system that fully complies with the functional specification
- Quality assurance team - verifies that the system complies with the functional specification through functional testing procedures
- System administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Customer Support - serves customers by providing product and service information that includes resolving product and service issues
- Audit and Compliance - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. Data coming into the environment is secured and monitored through the use of firewalls and an IPS (intrusion prevention system). Customer data is captured which is utilized by Options IT in delivering its IaaS - Options IT Platform Services System. Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority. Critical data is stored in encrypted format using software supporting the Advanced Encryption Standard (AES). The antivirus software is configured to scan workstations on a weekly basis. Additionally, vulnerability scans are performed on at least a monthly basis. Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS (intrusion detection system) alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. Teams are expected to adhere to the Options IT policies and procedures that define how services should be delivered. These are located on the Company’s intranet and can be accessed by any Options IT team member.

<u>Physical Security</u>

Options IT data centers are located within dedicated, proprietary data centers that are purpose-built for both facilities and security criteria. Physical access the data center premises is controlled by a combination of access-lists, photo identification, security cards and biometric data. Once inside the data center premises, Options IT equipment is secured from unauthorized physical access within dedicated suites requiring additional security clearance.

In addition to physical security within data center sites, equipment is logically secured with the authentication and authorization schemas relevant to each machine (for example, Windows Kerberos authentication on Windows machines, and Cisco authentication and authorization on networking equipment). This provides an important restriction on the activities that could be performed on equipment even if unauthorized physical access were possible.

Options IT is able, by prior arrangement, to provide access for Options IT customers to Options IT data centers in order to demonstrate the physical security of equipment. To gain physical access customers are required to sign visitor logs and be provided with an access badge that grants limited access to the data center facility.

The supporting infrastructure for the in-scope systems are hosted by the subservice organizations. As such, each subservice organization is responsible for the physical security controls for the in-scope system. Please refer to the ‘Subservice Organizations’ section below for additional controls details.

<u>Logical Access</u>

Options IT uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users’ authorized roles in access control lists. In the event incompatible responsibilities cannot be segregated, Options IT implements monitoring of one or more of the responsibilities. Monitoring is performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

Employees and approved vendor personnel sign on to the Options IT network using an Active Directory user ID and password. VPN, databases and operating systems are configured to enforce multi-factor authentication (MFA). Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords conform to defined password standards and are enforced through parameter settings in the Active Directory.

These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Options IT network are required to use a token-based MFA system. Employees are issued soft token access upon employment; this access is deactivated upon leaving employment. Vendor personnel are not permitted to access the system from outside the Options IT network.

The Options IT network is designed around carrier-grade, low-latency Arista and Cisco networking equipment which has both the reliability and the flexibility to support the split production, single logical network model that underpins the Options IT services. Options IT infrastructure is located within logical networks that are accessible to Options IT customers only through authorized channels, and Options IT customer networks are segregated and secured by means of IP access-lists which provide internal firewalling within the network. This ensures that Options IT customers are not able to route to other private network segments, or to the core network segments on unauthorized routes or protocols. A demilitarized zone (DMZ) is in place to isolate outside access and data from the entity's environment. Administration sub-networks are provided with sufficient routing access to administer both core and private network segments, and the administration sub-networks themselves are protected from unauthorized access from both internal and external sources through IP access-lists and external firewalling respectively. This design allows Options IT customers to leverage the resilience, reliability and functionality of the Options IT single logical network design, with confidence in the security and the data on the network, while also avoiding the high costs and reduced functionality associated with creating and duplicating new network topologies for each customer.

All aspects of network design, implementation, administration, security and performance tuning are managed by Options IT on behalf of Options IT customers in order to maintain full control and responsibility for the network. Therefore, Options IT retains full administrative control over networking components, and is not able to share or divest administration to Options IT customers.

Options IT's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency.

Management ensures Options IT's policies and procedures are communicated to new employees through a new hire checklist. The checklist is completed and filed for new employees. In addition, the ongoing performance and competence of employees is evaluated through the annual evaluation process.

Options IT's Management follows a standard exit procedure for personnel leaving employment. This procedure includes returning equipment, information assets, and removal of physical and logical access rights.

Computer Operations - Backups

Under the Options IT infrastructure, tape backups are an important part of data archiving and recovery but are viewed as a recovery mechanism of last resort. The Options IT “split-production” network design and operating model allows business critical data residing on Options IT servers to exist at multiple data center sites, and for data to be updated in near real time. In addition, intra-day snapshotting and roll-back technologies are used to provide “near-line” (nearly online) recovery for data that has been changed, deleted or corrupted on a primary server and subsequently replicated to other servers at other data center sites. These snapshot and roll-back technologies allow recovery of intra-day data from file servers without the need to resort to tape-based backups.

Tape backups are provided, however, as an important last line of defense against data loss caused by user action, error, or external events. As such Options IT retains exclusive control over tape backups and tape media. Data relevant to Options IT services is backed up to tape at the end of every day. For servers, full backups are run during each weekend, and differential backups are run at the end of each weekday.

These backup images are retained for three months before they are expired, and the tapes reused. Since month-end backups can contain data with special significance, full backups taken during the first weekend of every calendar month in respect of the previous month-end are retained for 7 years. Additional year-end backups are taken after the last business day of the calendar year and are also retained indefinitely.

Tapes are retained within the backup library at the relevant data center for a certain period. After this time, they are removed to secure offsite fireproof storage located in a geographically separate location from any data center site. This ensures that tapes are available for rapid restore as required, and that tapes are securely archived when their immediate need for restores is less likely.

Computer Operations - Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

Options IT monitors the capacity utilization of physical and computing infrastructure both internally and for customers to ensure that service delivery matches service level agreements (SLAs). Options IT evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to, the following infrastructure:

- Data center space, power and cooling
- Disk storage
- Tape storage
- Network bandwidth

Options IT has implemented a patch management process to ensure contracted customer and infrastructure systems are patched in accordance with vendor recommended operating system patches. Customers and Options IT system owners review proposed operating system patches to determine whether the patches are applied. Customers and Options IT systems are responsible for determining the risk of applying or not applying patches based upon the security and availability impact of those systems and any critical applications hosted on them. Options IT staff validate that patches have been installed and if applicable that reboots have been completed.

The supporting infrastructure for the in-scope systems are hosted by the subservice organizations. As such, each subservice organization is responsible for the environmental security controls for the in-scope system. Please refer to the ‘Subservice Organizations’ section below for additional controls details.

Change Control

Options IT maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Connectivity between Options IT networks and any third-party is secured by Checkpoint and Fortinet firewall appliances running Checkpoint and Fortinet firewall applications. Internet uplinks as well as connectivity to third-parties across private or managed circuits terminate on secured or firewall interfaces that are subject to Checkpoint and Fortinet management and IDS. This design ensures high, industry standard level of security from known external threats, and also provides flexibility required to support the wide array of services available within the Options IT network. Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by Options IT. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Authorized employees may access the system through from the Internet through the use of leading VPN technology. Employees are authenticated through the use of a MFA system.

Boundaries of the System

The scope of this report includes the IaaS - Options IT Platform System Services performed in the New York, New York; London, England; Hong Kong, China; Belfast, United Kingdom; Auckland, New Zealand; Toronto, Canada; and Singapore facilities.

This report does not include the data center hosting services provided by Cyxtera, Digital Realty Trust, Equinix, Iron Mountain, Telehouse, and Telstra.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization’s last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization’s last review.

Criteria Not Applicable to the System

All Common Criteria/Security and Availability criterion were applicable to the Options IT IaaS - Options IT Platform Services System.

Subservice Organizations

This report does not include the data center hosting services provided by Cyxtera, Digital Realty Trust, Equinix, Iron Mountain, Telehouse, and Telstra.

Subservice Description of Services

Cyxtera, Digital Realty Trust, Equinix, Iron Mountain, Telehouse, and Telstra provide data center hosting services. Options IT leverage the facility-related components and activities that support the implementation, maintenance, operation, and security of managed datacenter hosting services. This includes provision of power, cooling and ventilation, secure rack and telecoms hosting as well intelligent hands services.

Complementary Subservice Organization Controls

Options IT’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Options IT’s services to be solely achieved by Options IT control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Options IT.

The following subservice organization controls should continue to be implemented by Cyxtera to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Cyxtera		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical security policies and procedures are in place to guide personnel in the following areas: Data center access for employees, contractors, and visitors; security monitoring; security assessments and access activity reviews.
		Site authorizers are utilized to approve permanent access to the data centers.
		Security access controls (i.e., physical barriers and doors, card-controlled entry points, biometric scanning, video surveillance and/or manned reception desks) are utilized to protect areas that contain information and information processing facilities.

Subservice Organization - Cyxtera		
Category	**Criteria**	**Control**
		Control mechanisms are in place to limit physical access to restricted data center areas such as the raised floor, equipment rooms, transport areas, and critical power and mechanical infrastructure.
		Data center badge access requests for Company employees and contractors require a completed badge access request approved by site authorizers. Badge access requests for customers require a completed badge access request approved by an authorized customer representative.
		Data center security personnel undergo a certification process upon hire and annually thereafter to maintain awareness and help ensure adherence to current physical security policies and procedures.
		Data center access for Company personnel is revoked as a component of the employee termination process.
		Temporary access to the data centers for Company contractors must be pre-approved by a work order or ticket. Temporary access to data centers for customers requires prior authorization by the authorized customer representative.
		Customer-maintained access lists are utilized to identify customer representatives authorized to request permanent or temporary access to the data center(s) where the customer colocation space resides.
		Visitor logs are maintained for at least 90 days to document visitor activity at the data centers.
		Visitors are required to be escorted by an authorized Company employee or authorized customer representative at all times while in the data centers.
		Persons entering the data centers must present valid government-issued photo ID or display and use a valid Company photo access badge prior to entering the facility.
		CCTV surveillance video and/or ACS activity logs are retained for a minimum of 90 calendar days.
		Data center security personnel and the PSCC monitor access to the data centers 24 hours a day, seven days a week, using reports from the physical security access mechanisms, alarms, and CCTV video surveillance systems.
		Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises are controlled and, where applicable, are isolated from information processing facilities to avoid unauthorized access.
		An inventory of access badges and metal keys designated for loan to employees, customers, or contractors, as applicable by locations, is performed at least once per day to account for all badges and metal keys.

Subservice Organization - Cyxtera		
Category	**Criteria**	**Control**
		All shipments received at the data centers are stored in a physically secured location.
		Access to the shipping and receiving areas at the data centers is restricted to authorized personnel.
		The GRC team performs remote reviews of the data centers based on a threat vulnerability risk assessment on an annual basis to help ensure physical and environmental security policies and procedures are followed. Findings of noncompliance are reported to data center security personnel or facility management personnel for remediation.
		Badge access reviews are performed annually to help ensure that access to the data center facilities is restricted to authorized personnel.
Availability	A1.2	Environmental security policies and procedures are in place to guide personnel in the following areas: Equipment specifications and operating instructions; equipment inspections; preventative maintenance schedules (internal and external maintenance activities).
		A BMS is configured to monitor data center equipment including, but not limited to, the following: Fire detection and suppression systems, as applicable; HVAC units; generators, as applicable; electrical systems, as applicable.
		The BMS is configured to notify data center staff via on-screen and e-mail alerts when predefined thresholds are exceeded on monitored devices.
		Power management equipment is in place at each data center.
		Third-party specialists inspect power management systems according to a predefined maintenance schedule.
		Fire detection and suppression equipment is in place at each data center.
		Third-party specialists inspect fire detection and suppression systems on an annual basis.
		HVAC systems are in place at each data center.
		Third-party specialists inspect HVAC systems and water detection sensors, as applicable, according to a predefined maintenance schedule.
		The GRC team performs remote reviews of the data centers based on threat vulnerability risk assessment on an annual basis to ensure physical and environmental security policies and procedures are followed. Findings of noncompliance are reported to data center security personnel or facility management personnel for remediation.

The following subservice organization controls should continue to be implemented by Digital Realty Trust to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Digital Realty Trust		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical access controls are in place to restrict access to and within the data center facilities.
		Physical access requests are documented and require the approval of the site manager.
		A review of Digital Realty employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, notified, and removed.
		A termination notification ticket is completed by HR and physical access it revoked by the corporate security ream for Digital Realty employee and contractor terminations within one business day of termination.
		Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day.
		Surveillance cameras are in place to monitor and record access to and within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
		Digital surveillance systems are configured to retain video footage for the data centers for a minimum of 90 days.
Availability	A1.2	BMS applications are configured to monitor environmental systems and physical access systems and alert IT personnel when predefined thresholds have been met.
		Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
		The data centers are equipped with the following environmental protection equipment: • Fire detection and suppression equipment • UPS systems • Generators • CRAC/CRAH units
		Management retains the inspection report received from third-party specialists evidencing completion of inspection and maintenance of the following according to a predefined schedule: • Fire detection and suppression equipment • UPS systems • Generators • CRAC/CRAH units

Subservice Organization - Digital Realty Trust		
Category	**Criteria**	**Control**
		Site security personnel are assigned daily operational procedures and tasks that include environmental system monitoring.

The following subservice organization controls should continue to be implemented by Equinix to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Equinix		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical access control systems are in place to restrict access to and within the corporate facility and data center housing the facilities, backup media, and other system components such as firewalls, routers, and servers to properly authorized individuals.
		Procedures exist and are followed to established and make changes to physical access privileges for customers.
		Security personnel review a government issued ID prior to allowing off-site employees, visitors, customers, vendors, and contractors access to the facility.
		Procedures exist and are followed to establish and make changes to physical access privileges for employees.
Availability	A1.2	Fire detection and suppression equipment is in place at each facility.
		Scheduled maintenance procedures are performed to ensure that fire detection and suppression equipment is working properly.
		Power management equipment is in place for each facility.
		Scheduled maintenance procedures are performed to test and confirm the operation of the power management systems.
		Air conditioning and ventilation equipment is in place at each facility to ensure that humidity levels and the required temperature are maintained.
		Scheduled maintenance procedures are performed to ensure that the HVAC equipment and temperature and water detection sensors are working properly.
		Internal and external monitoring of environmental systems activity is performed through the use of BMS and 24x7 monitoring by facility engineers.
		Backup systems are in place to perform scheduled backups of production data at predefined times.
		Emergency procedures are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.

The following subservice organization controls should continue to be implemented by Iron Mountain to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Iron Mountain		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Physical security policies and procedures are in place to guide personnel in the following areas: • Data center access • Security monitoring • Security assessments and access reviews
		Physical access controls are in place to restrict access to and within the data center facilities.
		Surveillance cameras are in place to monitor and record access to and within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
		Digital surveillance systems are configured to retain video footage for the data centers for a minimum of 90 days.
		Access to the data centers is revoked as a component of the employee termination process.
		Visitors are required to provide government issued identification (ID) and sign a visitor’s log prior to gaining access to the facility.
		Customer equipment within the data centers is maintained in locked cages or cabinets.
		Physical access reviews are performed quarterly by data center management to ensure that access to the facility and data is restricted to authorized personnel.
		Visitors are required to provide government issued identification (ID) and sign a visitor’s log prior to gaining access to the facility.
		Surveillance cameras are in place to monitor and record access to and within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
		Physical access reviews are performed quarterly by data center management to ensure that access to the facility and data is restricted to authorized personnel.
Availability	A1.2	The data centers are equipped with the following environmental protection equipment’s: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units

Subservice Organization - Iron Mountain		
Category	**Criteria**	**Control**
		Management ensures that third-party vendors inspect the following environmental protection equipment at a predefined basis following manufacturer's recommendations and organizational standards to verify that the equipment is in proper working order: • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units
		Monitoring applications are configured to monitor the in-scope systems capacity levels and alert IT personnel when predefined system events are identified.
		A BMS is in place or facilities personnel perform manual walkthroughs to monitor the data centers' environments for predefined thresholds including, but not limited to, the following: • Temperature • Fire detection and suppression systems • HVAC units • Generators • Electrical systems
		Backups of production servers and databases are performed by operations personnel.
		Monitoring tools are configured to monitor backup systems to notify personnel if a job does not complete successfully.
		Business continuity plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.
		Contingency plans are tested on an annual basis.

The following subservice organization controls should continue to be implemented by Telehouse to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Telehouse		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	User entities are responsible for immediately notifying Gotham of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
		An ID card and biometric scan physical access control system is implemented within the perimeter of facilities and at the entry and exit points of sensitive areas within these facilities.
		Mantraps are used for controlling access to highly sensitive areas within the facility.

Subservice Organization - Telehouse		
Category	**Criteria**	**Control**
		All visitors are required to sign in and must be escorted by an entity employee when visiting the facility.
		The badge access system is configured to log successful and unsuccessful badge access attempts and the logs can be traced to a specific date, time, and badge.
		A video surveillance system is in place to monitor and record activity in areas including, but not limited to, the following: • Facility entrances and secure areas • Data center entrance • Throughout data center areas
		Two factor authentication (badge and biometric) is used to grant access to sensitive areas.
Availability	A1.2	Environmental protections have been installed including the following: • HVAC • UPS system • On-site backup generator • Redundant communication lines • Fire suppression • Smoke detectors • Fire extinguishers
		Operations personnel monitor the status of environmental protections during each shift.
		Environmental protections receive preventative maintenance on at least an annual basis.

The following subservice organization controls should continue to be implemented by Telstra to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - Telstra		
Category	**Criteria**	**Control**
Common Criteria/Security	CC6.4	Policies and procedures exist to ensure that physical access to facilities housing information systems is restricted to authorized personnel.
		Physical access to restricted areas of the facility is protected by walls with non-partitioned ceilings, secured entry points and/or manned reception desks.
		Physical access provisioning to facilities housing information systems required approval from appropriate personnel.
		Physical access deprovisioning to facilities housing information systems required approval from appropriate personnel.
		Physical account and access reviews are conducted on a quarterly basis. Corrective actions are taken where applicable.

Subservice Organization - Telstra		
Category	**Criteria**	**Control**
Availability	A1.2	Fire detection and suppression systems are implemented and tested at appropriate intervals.
		Temperature and humidity levels of data halls are monitored and maintained at appropriate levels.
		UPS and generators have been installed to support critical systems in the event of a power disruption.

Options IT management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Options IT performs monitoring of the subservice organizations controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

Options IT's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to Options IT's services to be solely achieved by Options IT control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Options IT.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Options IT.
2. User entities are responsible for notifying Options IT of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Options IT services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Options IT services.
6. User entities are responsible for providing Options IT with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Options IT of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.