Service Organization Controls 3 Report

Report on
Hong Kong Telecommunications Limited's
HKT Enterprise Cloud
Relevant to Security

For the period November 1, 2018 to October 31, 2019

Ernst & Young
22/F, CITIC Tower
1 Tim Mei Avenue
Central, Hong Kong

安永會計師事務所
香港中環添美道 1 號
中信大廈 22 樓

Tel 電話: +852 2846 9888
Fax 傳真: +852 2868 4432
ey.com

Report of Independent Accountants

To the Board of Directors of Hong Kong Telecommunications Limited:

We have examined the management's assertion that Hong Kong Telecommunications Limited, during the period November 1, 2018 to October 31, 2019, maintained effective controls to provide reasonable assurance that the HKT Enterprise Cloud was protected against unauthorized access (both physical and logical), use or modification, based on the criteria for Security principle set forth in the American Institute of Certified Public Accountants' ("AICPA") TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*. This assertion is the responsibility of Hong Kong Telecommunications Limited's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Hong Kong Telecommunications Limited's relevant security controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future period is subject to the risk that validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or deterioration in the degree of effectiveness of the controls.

In our opinion, Hong Kong Telecommunications Limited's management's assertion referred to above is fairly stated, in all material respects, based on the AICPA Trust Services Security Principle and Criteria.

Ernst & Young

10 February 2020
Hong Kong

Hong Kong Telecommunications Limited
http://www.hkt.com
39th Floor, PCCW Tower
Taikoo Place
979 King's Road
Quarry Bay, Hong Kong

Management's Assertion Regarding the HKT Enterprise Cloud Based on the AICPA Trust Services Principles and Criteria for Security

Hong Kong Telecommunications Limited ("HKT") has maintained effective controls over the security of its HKT Enterprise Cloud (the "cloud") to provide reasonable assurance that the HKT Enterprise Cloud was protected against unauthorized access (both physical and logical), use or modification during the period November 1, 2018 to October 31, 2019, based on the criteria for the security principle set forth in AICPA's TSP section 100, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Our attached Description of HKT Enterprise Cloud service identifies the aspects of the cloud covered by our assertion.

Hong Kong Telecommunications Limited

10 February 2020
Hong Kong

Description of HKT Enterprise Cloud service relevant to Security for the period November 1, 2018 to October 31, 2019

HKT Background

Hong Kong Telecommunications Limited ("HKT") is Hong Kong's premier telecommunications service provider. It serves the needs of the Hong Kong public and local and international businesses with a wide range of services including local telephony, local data and broadband, international telecommunications, mobile, and other telecommunications businesses such as customer premises equipment sale, outsourcing, consulting, and contact centers.

Description of Services

HKT Enterprise Cloud (the "cloud") is a carrier-grade cloud service which is available to customers in Hong Kong and Mainland China, powered by HKT's robust network infrastructure and facilities management expertise. It provides flexible, scalable and secure IT infrastructure to enterprises around the world. With the cloud, enterprises can deploy solutions on a cloud computing environment that provides compute power, storage and other application services over the Internet as their business needs demand. HKT affords enterprises the flexibility to employ the operating systems, application platforms and databases of their choice. Enterprises can enjoy faster time to market, and greater flexibility and scalability, while maintaining stringent service level agreements ("SLA"), as well as low skill-set investment and capital expenditure.

HKT offers private data network with fiber broadband Internet for its Cloud services so as to enable co-located customers to connect their own servers directly to the cloud, resulting in low-latency and stable connectivity. HKT provides a resource pool that enables enterprises to manage virtual infrastructure, such as CPU, storage, RAM and network, according to their needs. Enterprises gain the flexibility to administer and access their own equipment, while taking advantage of HKT network performance, security, and scalability.

The cloud contains several solution blocks, which includes the following:

- Cloud Computing Platform - provides computed resources for service subscriptions and specific service platform,
- Unified Network Infrastructure - is the core network architecture supporting the HKT Cloud Platform,
- Managed Service Platform – manages application performance, system stability and network trouble spots through network solution, and
- Network Connection Platform – provides network solutions supporting the high connectivity, availability and secure access to the cloud.

In Enterprise Cloud Service, there are 4 basic Service Packages, which are Starter Cloud Data Center Package, Advanced Cloud Data Center Package, Mission Critical Data Center Package and VMware Cloud Package. Each Service Package offer different level of SLA and bundled Valued Added Services to end customers.

Components of the platform

The following sections define each of these components comprising the platform:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, application, and utilities)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)
- Data (files, database, and tables)

Infrastructure – the physical and hardware components of the Cloud including facilities, equipment, and networks.

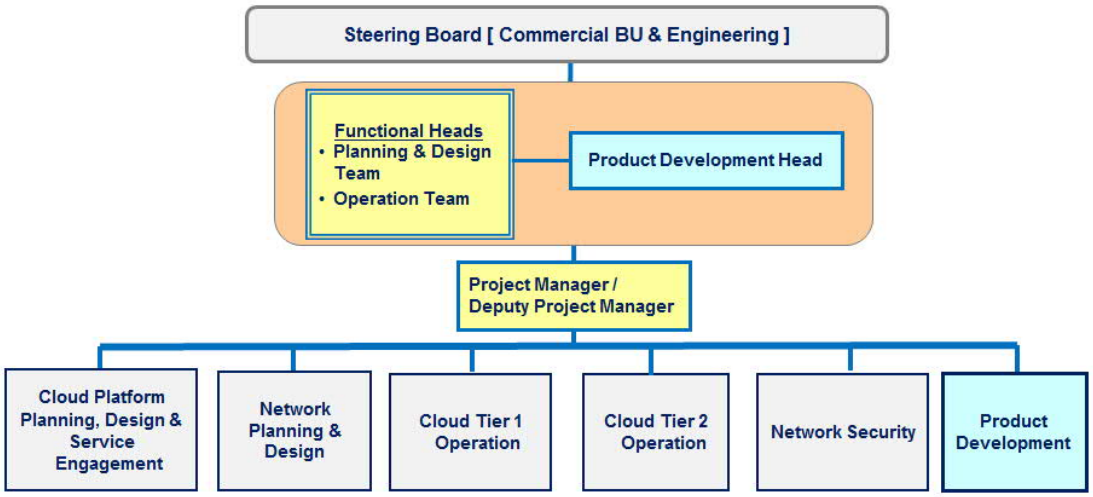
HKT infrastructure includes HKT network backbone consisting of multiple layers of routers, switches and load balancers. HKT does not control customer-specific hardware, operating systems, databases, applications, or any other content loaded on the customer hardware. The Cloud services is hosted on a Virtual Data Center ("vDC"), an Infrastructure-as-a-Service ("IaaS") solution providing a collection of virtualized computing, storage, networking, security and valued-added services within separate logical partitions in a multi-tenant infrastructure. Security is provided within the virtualized environment using secure multiple server segmentation ensuring each vDC is fully isolated from other vDCs.
HKT configures the customer site on its own vDC which consists of different resources with different SLA (i.e. different cloud packages) that are based on each individual customer's specifications. HKT is responsible for setting up each individual customer's environment, providing network connectivity and power for the environment, and managing the environmental safeguard systems. Once the customer environment has been set up, HKT turns over the environment to the customer who is then responsible for building/staging its own infrastructure.

Software – the programs and operating software of the System including systems, applications, and utilities.

HKT does not access customer's systems at the operating system, database, or application levels. As part of the HKT service, when a customer is not able to be on-site at the HKT data centers, HKT provides hands-on technical support should the customer require technical assistance such as a system reboot or a hardware replacement.

People – the personnel involved in the operation and use of the System including developers, operators, users, and managers.

HKT organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled and monitored. HKT has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting for managing the Cloud services.
HKT has an established organization structure with defined roles and responsibilities.



The following teams are involved in the Cloud services provided by HKT:

Team Name	Responsibility
Cloud Platform Planning, Design & Services Management	HKT Enterprise Cloud platform planning and design, integration of services, platform sizing and capacity monitoring.
Network Planning & Design	Equipment procurement, solution integration, testing and capacity planning of the Network supporting the Cloud's services. Review on the network design to determine if the current network design meets business needs.
Cloud Tier 1 Operation	Day-to-day operation and security of the data center including physical access administration, assistance, oversight, and customer interface on physical security issues, policies, and procedures.
Cloud Tier 2 Operation	Day-to-day operation and network and security of the Cloud including monitoring security alarms on Cloud and perform troubleshooting, monitoring the Cloud's services for compliance with service level agreement commitments and configuration of the customer site.
Network Security	Administration, monitoring, and maintenance of HKT infrastructure and networking components as they relate to the Cloud services including routers and IP assignment and configuration. Oversight on security issues, policies and procedures. Perform risk assessment on the Cloud's security and identify controls on the identified risk areas.

Team Name	Responsibility
Product Development	Plan, develop and manage end-to-end service delivery platform, process, skills and tools for new product roll-out. Evaluate technology trends, customer feedback, market trends and competitive activities to formulate product development plan for Cloud Computing Services. Manage the on-going product operations, including but not limited to quality assurance, cost-improvement, and product enhancement to ensure competitiveness of Clouds' product in the market.

Procedures – the automated and manual procedures involved in the operation of the System.

The Company's employees adhere to HKT's corporate policies that define how services should be delivered. The policies are located on HKT's intranet and can be accessed by the Company's employees.

Data – the information used and supported by the System.

HKT does not manage or input data into customer systems and is not responsible for the accuracy or completeness of customer data. Customer data necessary to provide the services within the boundaries of the Cloud is managed in accordance with the relevant data protection and other regulations, with any specific requirements specified in the customer contracts.

Communication

Management of HKT is committed to maintaining effective communication with all personnel and customers. To help align HKT strategies and goals with operating performance as it relates to customers, policies and procedures for problem and incident, change management, risk management for HKT Enterprise Cloud is in place to ensure the internal / external communication with concerned party are effective, well organized and in a timely manner. Also, the Cloud services details including scope, purpose and design of the Cloud services, key organization and system support functions, processes, and roles and responsibilities for the Cloud services are made available to HKT's employees through HKT's intranet to ensure the employees supporting the Cloud services are clear on their role and responsibility on the Cloud services delivery.
The Cloud services description including the security commitments of the Cloud Service are available for potential customers during the cloud service introduction session. Customer obligations are presented to customers in combination with the Terms and Conditions and Acceptable User Policy ("AUP"), which specifies customers' responsibilities in using the Cloud's services, as part of the customer contract. Customer obligations and responsibilities are reinforced through the VMware VCloud Director (Client Portal for VMware) and the AUP is also available on VMware VCloud Director for customers' reference. Customers must agree to comply with the requirements and violations are investigated.
HKT has also provided a report hotline to customer for reporting problems and incidents to HKT in case of any security failure or incidents occurred so that the problem / incident could be handled properly and timely and minimize the services performance impact to the

customers.
Suspected information security incidents shall be reported to the Security Manager. The Risk Management & Compliance Group maintains primary responsibility for liaison with external law engagement agencies for security incidents.

Risk Assessment

HKT employs formal risk assessment procedures. It has a risk management policy and procedure to identify potential threats that would affect the HKT Enterprise Cloud service. A master list of the HKT's system components is maintained by the Cloud Project Team, which accounts for additions and removals of system components, so that all system components are included in the risk management process and risks could be appropriately identified.

HKT has defined a formal risk management process that specifies risk tolerances and the process for evaluation risks based on identified threats and the specified tolerances. Risk assessment on HKT Enterprise Cloud is conducted annually and is reviewed by the Engineering Network Service team. Risk assessment is also conducted annually for the three data centers hosting the Cloud services, including Junk Bay (JBY) data center, Lockhart (LKT) data center, and SkyExchange (IAC) data center. The risk assessment process includes identifying, prioritizing, and ranking risks at activity level on HKT Enterprise Cloud with the defined risk evaluation process and ratings. Criteria used to rank risks include, but are not limited to, technological complexity and dependencies, security vulnerabilities and process impact on the HKT’s reputation. All risks have been reviewed by management and risk mitigation action is done to lower the risk to an acceptable level.

The design philosophy for the HKT enterprise cloud is to build up resilience such that in case any individual incident occurs, HKT enterprise cloud could remain service with the resilience node.

Monitoring

Management of HKT has implemented a division of roles and responsibilities, which limits the ability of a single individual to subvert critical processes. This segregation of duties increases control over processes that may impact customer systems. There are procedures in place to help ensure that personnel perform only those duties related to their positions.
HKT used tools, including Cacti, SNMP protocol, McAfee Endpoint Security and Trend Micro Deep Security Manager, to perform monitor system performance, security threats, resource utilization needs, and unusual system activities of the infrastructure of HKT Enterprise Cloud, such that incidents would be detected in a timely manner. Once incidents and abnormal system performance are detected, Cloud Tier 1 Operation team and Cloud Tier 2 Operation team will receive email alert and follow the defined incident management policy and procedure to notify the concerned party and perform restoration action accordingly to minimize the impact to HKT Enterprise Cloud Service.
Bi-weekly meetings are held within the Cloud Services Team to discuss any issues on the Cloud's services and review the system performance metrics pertaining to system performance and availability.

Physical and Information Security

HKT has established security policies and practices such that HKT assets are safeguarded and access to HKT systems, networks, resources, and data is secured.

The cloud's data center is complied with the requirement of ISO/IEC 27001 on Information Security Management. Access to the data centers are limited to authorized individuals based on job function and responsibility within the data center. Visitors to the data centers are required to sign in and out on the visitor log and must be escorted by authorized personnel.

Environmental safeguards are the protective measures utilized to help protect physical surroundings from damaging elements, such as fire, water, smoke, and electrical surges, spikes, and outages so as to further safeguard customer's information assets located within the facilities. They are implemented and monitored throughout the data centers to provide for the safety of the employees, HKT's property, and other pertinent physical elements within the facility.

Logical access is controlled via separate authentication domains in which limited access is granted to the administration network and supporting tools for the cloud services. Users are only provided with access to the applications that they have been specifically authorized to use. Accounts on administration network and the cloud's supporting tools are managed by the established account handling procedures. Unique user IDs and two-factor authentication technique are in place for customer's identification and authentication when logging into the cloud's network and applications.

The access review policy is in place that management shall review users' access rights at regular intervals to determine if the access rights are appropriately granted in accordance with the staff's roles and responsibilities.

The cloud's Firewall Hardening Guideline defines the principles for the hardening of firewall of the cloud. Firewall protection is provided by industry standard firewall appliance equipment.

The equipment is configured to protect against unauthorized access to internal HKT resources.

HKT has also implemented a program for spam and virus protection that consists of software implemented and configured on servers and workstations. Periodic reviews of the software installation on staff's workstation / laptop were performed to ensure only authorized and registered software were installed.