Cloud service provider disclosure

The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, indicate accordingly in the remarks.

Cloud Service Provider Contact Information
Company name: Tata Communications International Pte Ltd Primary address: 35 Tai Seng street, #06-01, Singapore 534103 Web address: http://www.tatacommunications.com/ Contact name: Shaji Firoz Contact number: +65-66326989
Certification Body Contact Information
Company name: TÜV SÜD PSB Pte Ltd _____ Web address: ___ http://www.tuv-sud-psb.sg _____ Contact name: ___ CHAY-LEE, Swee Gee _____ Contact email: __ swee-gee.chay@tuv-sud-psb.sg ___
Cloud Service Provider Background
Overview of service offering: Tata Communications' Cloud suite is a flexible, cost-effective cloud computing solution that lets customers instantly provision virtual machines, storage and network infrastructure on a pay-as-you-go basis with flexible payment options, security, guaranteed service levels and 24/7 technical support. Tata Communications Cloud suite comprises of IZO™ Private Cloud & IZO™ Cloud Storage, Virtual Private Data Center its flagship services that are made available to its customers through a self-service web portal, which acts as a single-pane-of-glass, for all IT resources deployed by the customer. Service model: ☒ Virtual machine instances owned by the user ☒ Network facilities ☒ Compliance with applicable standards Deployment model: ☒ Private cloud ☐ Community cloud ☒ Hybrid cloud ☐ Public cloud

Tier:			
	☐ Level 1		
	☒ Level 2		
	☐ Level 3		
No.	**Criteria**	**Description**	**Remarks**
		Legal and Compliance	
1.	Right to audit	The user has the right to audit: ☒ Virtual machine instances owned by the user ☒ Network facilities ☒ Compliance with applicable standards ☒ Technical controls ☐ Policies and governance ☒ Data centre facilities ☐ Others _____ ☐ None Regulators recognised by Singapore law have the right to audit: ☐ Virtual machine instances owned by the user ☐ Network facilities ☐ Compliance with applicable standards ☐ Technical controls ☐ Policies and governance ☒ Data centre facilities ☐ Others _____ ☐ None	Customers can perform their own compliance audit on their virtual infrastructure (servers, network, storage, etc.). Customer can request one audit per calendar year limited to Tata ommunication cloud services and with a minimum of 15 days advanced notice. Any information, document, reports are available under Tata Communications terms of non-disclosure agreement. If customer wants 3rd party to perform audits customer to ensure 3rd party signs Tata Communications terms of non-disclosure agreement. Any additional audits would be on chargeable basis and on discretion of Tata Communications. Penetration Test, and Vulnerability scanning reports are provided to auditors upon request as part of audit requirements. Reports are provided with proper justification, investigation. All reports, documents are available under the terms of non-disclosure agreement.

		Audit / assessment reports that can be made available on request: ☒ Penetration test ☐ Threat and vulnerability risk assessment ☒ Vulnerability scan ☐ Audit reports (e.g. Statement on Standards for Attestation Engagements (SSAE) No. 16, Reporting on Controls at a Service Organisation)	Customers who would like to conduct Penetration test / Vulnerability Assessment of their Application / public facing interfaces can perform such testing at their end with prior approval from Tata Communications and based on agreed Tata Communication MSA. Requests for Scan / penetration testing should be submitted with a minimum of 15 days advanced notice.
2.	Compliance	The following guidelines / standards / regulations are adhered to: ☒ Singapore Personal Data Protection Act ☒ ISO / IEC 27001 ☐ ISO 9000 ☒ ISO / IEC 20000 ☒ CSA Open Certification Framework ☒ PCI-DSS ☐ Others _____	Tata Communications is certified for ISO/IEC 27001:2013, ISO/IEC 20000:2011 for its Managed Hosting and Security Services and undergoes independent assessments on an annual basis. CSA Self assessment - Consensus Assessments Initiative questionnaire (CAIQ) v3.0.1 - https://cloudsecurityalliance.org/star-registrant/tata-communications/ PCI-DSS is under progress
Data Control			
3.	Data ownership	All data on the cloud service is owned by the cloud user except for: Configuration files and log data related to cloud infrastructure platform. The cloud User retains the ownership on the derived data or attributes of cloud usage except for the following: ☐ Advertising or marketing ☒ Statistics analysis on usage ☐ Others_____	
4.	Data retention	Data deleted by the user is retained as follows: ☐ Minimum data retention period is: _____ ☒ Maximum data retention period is: 7 Days	Tata Communications provide customers with the ability to delete their data. Customers may extract and/or delete

		☐ Deleted immediately	their data at any time.
		Log data is retained for a period of:	On log data retention, this varies based on type of logs.
		☒ Minimum data retention period as follows: 3 months	Logs controlled by the user are retained for whatever period the user sets. Cloud platform logs are retained for 3 months.
		☒ Maximum data retention period is: 1 year	
		☐ Not retained	
		User data is retained for a period of:	Logs detail are only specific to Cloud infrastructure.
		☐ Minimum data retention period is: _____	Log data for customer owned virtual servers is the responsibility of the customer.
		☒ Maximum data retention period is: 7 days	
		☐ Not retained	
		The following types of data are available for download by the cloud user:	Customer is responsible for transfer/delete backup of data and this may be carried out within 15 days of termination coming into effect and hence retained for 15 days maximum.
		☐ Log data	
		☐ Other _____	
5.	Data sovereignty	The primary data locations are:	Tata Communications provides customers with the flexibility to restrict connections based on IP Address, Certificate Based authentication and other connection filters.
		☒ Singapore	
		☐ Asia Pacific _____	
		☐ Europe_____	
		☐ United States	Tata Communications provides its customers to choose the data center where their infrastructure should be hosted. Customers can choose their data locations and their data will stay within that location they specify.
		☐ Other _____	
		The backup data locations are:	
		☒ Singapore	
		☐ Asia Pacific_____	
		☐ Europe_____	
		☐ United States	Five Countries are: US, UK, India, Singapore & Hong Kong
		☐ Other _____	
		No. of countries in which data centres are operated: 5 (five)	
		The user's data stored in the cloud environment will never leave the locations specified in item 5:	

		☒ Yes	Data will not be moved across data centers /geographies without the consent of the customer.
		☐ Yes, except as required by law	
		☐ Yes, except as noted: required by the customer	
		☐ No	
		User's consent is required prior to transferring data to a location not specified in item 5 or a third party:	
		☒ Yes	
		☐ Yes, except as required by law	
		☐ Yes, except as noted: _____	
		☐ No	
		Note: Cloud users are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. In addition, users should understand the risks associated with relevant laws that may allow for law enforcement or other government access to data in-transit or storage with Cloud Service Providers.	
6.	Non-disclosure	☒ Non-disclosure agreement template can be provided by Cloud Service Provider	
		☐ Cloud Service Provider may use customer's NDA (pending legal review)	
Provider Performance			
7.	Availability	The committed network uptime is: ☒ 99.9% ☐ Varies according to price plan The committed system uptime is: ☒ 99.9% ☐ Varies according to price plan The cloud environment has the following single points of failure: ☐ _____ ☒ none	Customer network is excluded and are advised to have redundant links. Customer are encouraged to have backup/recovery and opt for different Data Center as part of solution. For detailed service level and uptime commitments please refer to Service schedule. Based on the customer requirement Uptime committed can be increased.
8.	BCP / DR	☒ Disaster recovery protection	Tata Communications Offers cloud services from Multiple data

		☒ Backup and restore service ☒ User selectable backup plans ☒ Escrow arrangements ☐ No BCP / DR is available ☐ RPO_____ ☐ RTO_____ ☒ Others, please specify: DR is an optional service and RTO & RPO are defined asper the Customer requirements	Center locations across the globe. DR is an optional service which Customers have the flexibility to choose any of the data center locations depending on their Business Continuity requirements and RTO/RPO. Based on customer's requirement, Tata Communications can design and incorporate solutions to support their RTO/RPO.
9.	Liability	The following terms are available for the users on failure of the provider to meet the service commitment: ☒ Network failure Liability: Service Credit ☒ Infrastructure failure Liability: Service Credit ☒ Virtual machine instance failure Liability: Service Credit ☐ Migrations Liability:_____ ☒ Unscheduled downtime Liability: Service Credit ☐ Database failure Liability:_____ ☐ Monitoring failure Liability:_____	Service credits would be based on service schedule/SLA agreed.
Service Support			
10.	Change management	The Cloud Service Provider has established the following for changes, migrations, downtime, and other potential interruptions to cloud services: ☒ Communication plan and procedures for proactive notification	

		☒ Assistance in migration to new services when legacy solutions are discontinued	
		☒ Ability to remain on old versions for a defined time period	
		☒ Ability to choose timing of impact	
11.	Self-service provisioning and management portal	Provide self-service provisioning and management portal for users to manage cloud services: ☒ Yes ☐ No If yes, describe the functions of the self-service provisioning and management portal provided: ☒ Allow role-based access control (RBAC) ☒ Manage resource pools (e.g. VMs, storage, and network) and service templates ☒ Track and manage the lifecycle of each service ☒ Track consumption of services ☐ Others: _____ _____	Only applicable for IZO Private cloud customer. For VPDC self-service portal is not provided.
12.	Incident and problem management	Delivery mode of support: ☒ Access via email ☒ Access via portal ☒ Access via phone support ☒ Direct access to support engineers Availability of support: ☒ 24 x 7 ☐ During office hours support, please specify the hours of operations: _____ ☐ After office hours support, please specify the hours of operations: _____ Service response time: _____ The following are available to users upon request: ☐ Permanent access to audit records of customer instances ☒ Incident management assistance	

		Incident response time: Based on severity of incident	
		Mean time to repair on detection of faults: Based on severity of incident	
13.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☒ Pay per usage _day & month__ (up to per day/month for compute/storage for IaaS ☒ Fixed pricing_____(up to yearly/monthly/daily) ☐ Other pricing model_____ ☐ Not disclosed ☒ Available billing history: 12 Months	
14.	Data portability	Importable VM formats: VmWare, HyperVisor, KVM Downloadable formats: _____ Supported operating systems: _____ Language versions of supported operating systems: Windows, All versions of Linux Supported database formats: MSSQL, MySQL API: ☐ Common _____ ☐ Customised _____ Upon service termination, data is available through: ☐ Physical media ☒ Standard methods as described above ☐ Other methods _____ _____	Media to be provided by customer
15.	Access	Type of access to the service is through: ☒ Public access ☒ Private access (e.g. VPN, dedicated link) ☐ IPv6 access is supported ☐ Other access methods _____	

		_____ _____ Public access speed (shared bandwidth) in Mbps: 1024 _____	
16.	User management	☒ Identity management ☒ Role based access control ☐ Federated access model ☒ Integration with Identity management solutions ☐ Others_____	Identity and Role based management for IZO private cloud is available for self-service portal for cloud administration. Identity management can be of choice of customer and integration to self-service portal is allowed through APIs. Choice of identity management for User management for the provisioned VM server is the responsibility of the customer and is based on customer solution.
17.	Lifecycle	The cloud user may select the following for service upgrades and changes: ☒ Automatic provisioning ☒ User customisable provisioning	
Security Configurations			
18.	Security configuration enforcement checks	Security configuration enforcement checks are performed: ☒ Manually ☐ Using automated tools How often are enforcement checks being performed to ensure all security configurations are applied? One time upon initial configuration	Hypervisor and Management network supporting the delivery of service to customers is monitored for vulnerabilities. Security configuration of the customer's Guest OS/application is in the responsibility of the customer
19.	Multi-tenancy	☐ Distinct physical hosts ☐ Distinct physical network infrastructure ☒ Virtual instance grouping ☒ User definable security domains ☒ User customisable firewall ☒ User definable access policies	Tata Communications provide dedicated private and virtual multi-tenant cloud environment and solution.
Service Elasticity			

20.	Capacity elasticity	The following capacity elasticity options are available: ☒ Programmatic interface to scale up or down ☐ Mean time to start and end new virtual instances _____ ☐ Alerts to be sent for unusual high usage ☐ Minimum performance during peak periods_____ ☐ Minimum duration to scale up computing resources _____ ☐ Minimum additional capacity guaranteed per account _____ (number of cores and GB memory)	
21.	Network resiliency and elasticity	The following network resiliency and elasticity options are available: ☒ Redundant Internet connectivity links ☐ Redundant Internal connectivity ☒ Selectable bandwidth up to 1024 Mbps ☒ Maximum usable IPs _____ ☐ Load balancing ports_____ ☐ Load balancing protocols_____ ☒ Anti-DDOS protection systems or services ☐ Defence-in-depth mechanisms, please specify: _____ _____ _____ ☒ Network traffic isolation, please specify: Each customer has a separate Firewall Instance which is isolated by VLAN. ☐ Shared or dedicated bandwidth, please specify: _____ Based on customer requirements ☐ QoS traffic control services ☐ Alerts to be sent for unusual high usage ☒ Minimum performance during peak periods: committed Bandwidth ☐ Minimum period to scale up network throughput _____	Customer have choice of taking more bandwidths. By default one IP per Virtual Machine. Based on customer requirements, more IPs can be provided.
22.	Storage redundancy and elasticity	The following storage redundancy and elasticity options are available: ☒ Redundant storage connectivity links within each data centre	

		☐ Redundant storage connectivity links between data centres belonging to the same cloud	
		☒ Storage traffic isolation, please specify: Volume level isolation for each customer	
		_____	
		☒ Shared or dedicated storage network bandwidth, please specify: Shared	
		☐ Quality of service storage traffic control services	
		☐ Maximum storage capacity for entire cloud, please specify:	
		_____	
		☒ Maximum storage capacity for single user, please specify: Depends upon customer requirement	
		☒ Maximum expandable storage, please specify: Depends upon customer requirement	
		☐ Alerts to be sent for unusual high usage	
		☐ Minimum storage I / O performance during peak periods	
		_____	
		☐ Minimum period to scale up storage I / O throughput	
		_____	