Write

Read **SS 584 MTCS** Self Disclosure

	Legal & 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 As defined in customer contract
		☐ 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
		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)
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 FedRAMP, IRAP, SSAE 16 SOC 1 Type 2, SOC 2 Type 2
	Data Control	
3	**Data ownership**	All data on the cloud service is owned by the cloud user except for: N/A, ServiceNow customers own all data within their
		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: Backups are retained for 28 days maximum. ServiceNow does not archive backups for retention.
		☐ Deleted immediately
		Log data is retained for a period of:
		☑ Minimum data retention period as follows: ServiceNow retains all audit log data for 90 days online
		☐ Maximum data retention period is:
		☐ Not retained
		User data is retained for a period of:
		☐ Minimum data retention period is:
		☑ Maximum data retention period is: ServiceNow customers are responsible for management of their data, as such it is the customer's responsibility to manage data retention according to their own
		☐ Not retained
		The following types of data are available for download by the cloud user:
		☑ Log data
		☑ Other ServiceNow customers own all data within their instance and can download data as required.
5	**Data sovereignty**	The primary data locations are:
		☑ Singapore

	☑ Asia Pacific	Hong Kong							
	☐ Europe								
	☐ United States								
	☐ Other								
	The backup data locations are:								
	☑ Singapore								
	☑ Asia Pacific	Hong Kong							
	☐ Europe								
	☐ United States								
	☐ Other								
	No. of countries in which data centres are operated:	10							
	The user's data stored in the cloud environment will never leave the locations specified in item 5:								
	☐ Yes								
	☑ Yes, except as required by law								
	☑ Yes, except as noted:	ServiceNow stores customer data in its data centers hosted by third party providers. ServiceNow customers designate the physical region in which their data will be							
	☐ 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.....								
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**	For each cloud service offered, CSP should disclose relevant numbers) The committed network uptime is:								
	☑	99.8							
	☐ Varies according to price plan								
	The committed system uptime is:								
	☑	99.98							
	☐ Varies according to price plan								
	The cloud environment has the following single points of failure:								
	☐								
	☑ None								
8 **BCP / DR**	☑ Disaster recovery protection								
	☑ Backup and restore service								
	☐ User selectable backup plans								
	☑ Escrow arrangements								
	☐ No BCP / DR is available								
	☑ RPO	1 hour							
	☑ RTO	2 hours							
	☐ Others, please specify:								
9 **Liability**	The following terms are available for the users on failure of the provider to meet the service commitment:								
	☐ Network failure								
	Liability:								
	☐ Infrastructure failure								
	Liability:								
	☐ Virtual machine instance failure								
	Liability:								
	☐ Migrations								
	Liability:								
	☐ Unscheduled downtime								
	Liability:								
	☐ Database failure								
	Liability:								

		☐ Monitoring failure							
		Liability:							
	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							
		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:							
12	**Incident and problem**	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:							
		Mean time to repair on detection of faults:							
13	**Billing**	The following billing modes are available (please elaborate granularity of charges and measurements)							
		☐ Pay per usage (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per user per hour/day/month/year for SaaS)							
		☐ Fixed pricing (to yearly/monthly/daily)							
		☑ Other pricing model Refer to your customer contract for pricing mode							
		☐ Not disclosed							
		☐ Available billing history: hs							
14	**Data portability**	Importable VM formats: N/A, ServiceNow does not use virtual machines in it's environment.							
		Downloadable formats: https://docs.servicenow.com/use/reporting/reference/r_ReportOutputFormats.html							
		Supported operating systems: N/A, https://docs.servicenow.com/bundle/helsinki-release-notes/page/release-notes/servicenow-platform/generally-supported-browsers-rn.html							
		Language versions of supported operating systems:							
		Supported database formats:							
		API:							
		☑ Common http://wiki.servicenow.com/index.php?title=Web_Services#gsc.tab=0							
		☑ Customised http://wiki.servicenow.com/index.php?title=Web_Services#gsc.tab=0							
		Upon service termination, data is available through:							
		☑ Physical media							
		☑ Standard methods as described above							
		☑ Other methods Per the standard contract (MLA) with ServiceNow, at the termination of a business relationship between							
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 encrypted TLS web interface							
		Public access speed (shared bandwidth) in Mbps:							
16	**User management**	☑ Identity management							
		☑ Role based access control							
		☑ Federated access model							
		☑ Integration with Identity management solutions							
		☑ Others ServiceNow provides a SaaS offering to the customer. The responsibility for access management of the customer's ServiceNow application instance resides with the							
17	**Lifecycle**	The cloud user may select the following for service upgrades and changes:							
		☑ Automatic provisioning							
		☑ User customisable provisioning							
	configuration								
18	**configuration**	Security configuration enforcement checks are performed:							
		☑ Manually							
		☑ Using automated tools							
		How often are enforcement check being performed to ensure all security configurations are applied?							
19	**Multi-tenancy**	☑ Distinct physical hosts							
		☑ Distinct physical network infrastructure							
		☐ Virtual instance grouping							
		☑ User definable security domains							
		☑ User customisable firewall							
		☑ User definable access policies							
	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 up to 2 hours							
		☑ Alerts to be sent for unusual high usage							
		☐ Minimum performance during peak periods							
		☑ Minimum duration to scale up computing resources Computing resources scale on requirement of instances							
		☑ Minimum additional capacity guaranteed per account minimum capacity is provided through instance sizing							
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 ____ Mbps	External BW up to 1 Gbit/s (redundant)						
		☑ Maximum usable IPs	513 public addresses per site in each of HKG / SIN						
		☑ Load Balancing Ports	80, 443						
		☑ Load balancing protocols	http, https						
		☑ Anti-DDOS protection systems or services							
		☑ Defence-in-depth mechanisms, please specify:	Border filtering, Firewall, and Application Delivery Controller						
		☑ Network traffic isolation, please specify:	All traffic is isolated on a per-VLAN basis based on service						
		☑ Shared or dedicated bandwidth, please specify:	Shared						
		☐ QoS traffic control services							
		☑ Alerts to be sent for unusual high usage							
		☐ Minimum performance during peak periods							
		☑ Minimum period to scale up network throughput	Depends on location of network constrainment						
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: Backup traffic is isolated and has its own network							
		☐ Shared or dedicated storage network bandwidth, please specify:							

	☐ Quality of service storage traffic control services								
	☑ Maximum storage capacity for entire cloud, please specify:	40+ Petabytes and constantly increasing							
	☑ Maximum storage capacity for single user, please specify:	4TB limit per instance per contracts							
	☑ Maximum expandable storage, please specify:	10+ TB and requires custom contract							
	☐ 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								