iTSC
Information Technology Standards Committee

SGTECH
WHERE TECH MEETS

Procuring & Implementing Cloud Services from Cloud Service Providers (CSPs)

Tips And Best Practices For Cloud Services Customers (CSCs)

Version 1.0

Prepared By	Tao Yao Sing, Member, MTCS Working Group, CCS TC/ITSC
Reviewed & Edited By	SGTech Cloud & Data Chapter Exco (Suresh Agarwal, Raju Chellam, Vincent Lee, Abhishek Pradhan, Jonathan Kok)
Approved By	SGTech Cloud & Data Chapter Chair, Gunasekharan Chellappan
Date	16 November 2021

CONTENTS

1. Background

1.1 General

Cloud computing has gained significant momentum and popularity with the advent of critical enabling technologies in distributed systems, cluster computing, grid computing, virtualisation, web 2.0, and service orientation. Most businesses, including regulated industries, embrace a utility-based computing model. Many consumers are being served through "clouds" with popular services such as Gmail, Google Maps, Facebook, Twitter, YouTube, etc. However, the security and resiliency risks remain the key concerns of many Cloud Service Customers (CSCs) who source cloud services from the Cloud Service Providers (CSPs).

1.2 Audience

The target audience for this document is the CSC. It complements the Singapore Cloud Security Standard SS584 – Specifications for Multi-Tiered Cloud Computing Security. CSPs provide visibility and clarity of their cloud services' security provisions to match CSC's needs better.

1.3 Normative Reference

The following referenced documents are indispensable in the understanding of this guideline. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

SS 584: Specification for Multi-Tiered Cloud Security (MTCS).
TR 62: Guidelines for Cloud Outage Incident Response (COIR).

1.4 Cloud Computing Fundamentals

1.4.1 What is Cloud Computing

Cloud computing is a utility-based model that enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources. These can be networks, servers, storage, applications and services that can be rapidly provisioned and released with minimal management effort or service provider interaction as specified in NIST SP800-145.

1.4.2 Cloud Computing Service Models

There are three fundamental service models in cloud computing defined in NIST SP800-145 and excerpted from MTCS SS584.

1.4.2.1 Software-as-a-Service (SaaS)

The capability provided to the CSC is to use the CSP's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g. web-based email), or a program interface. The CSC does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

1.4.2.2 Platform-as-a-Service (PaaS)

The capability provided to the CSC to deploy on the cloud infrastructure customer-developed or acquired applications created using programming languages, libraries, services and tools supported by the CSP. The CSC does not manage/control the underlying cloud infrastructure, including network, servers, operating systems, or storage, but retains controls over deployed applications and possibly configuration settings for the application-hosting environment.

1.4.2.3 Infrastructure-as-a-Service (IaaS)

The capability provided to the CSC to provision processing, storage, networks, and other fundamental computing resources where the CSC can deploy and run arbitrary software, including operating systems and applications. The CSC does not manage/control the underlying cloud infrastructure but controls the operating systems, storage and deployed applications, and limited control of select networking components (e.g. host firewalls).

1.4.3 Cloud Deployment Models

Besides these service models, four deployment models are commonly seen in Cloud computing as defined in NIST SP800-145 and excerpted from MTCS SS584. The bulk of CSCs has adopted public cloud services. However, as CSCs are becoming more sophisticated and increasingly more competent technically, hybrid cloud models have become popular in recent years.

1.4.3.1 Private Cloud

The cloud infrastructure is provisioned exclusively by a single organisation/CSC comprising multiple users (e.g. business units). It may be owned, managed and operated by the organisation, a third party, or some combination, and it may exist on or off-premises.

1.4.3.2 Community Cloud

The cloud infrastructure is provisioned for exclusive use by a community of CSCs from organisations with shared concerns (e.g. mission, security, policy and compliance considerations). It may be owned, managed and operated by one or more organisations in the community, a third party, or some combination, and it may exist on or off-premises.

1.4.3.3 Public Cloud

The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic or government organisation, or some combination thereof. It exists on the premises of the CSP.

1.4.3.4 Hybrid Cloud

The cloud infrastructure consists of two or more distinct cloud infrastructures (private, community or public) that remain unique entities. However, they are bound together by standardised or proprietary technology enabling data and application portability (e.g. cloud bursting for load-balancing between clouds).

1.4.4 Charging Schemes (Cost Characteristics)

The charging schemes vary across different CSPs for cloud service and deployment models. Generally, CSCs pay according to the cloud resources consumed. Still, sometimes CSCs may also have to pay separately for network bandwidth, data transfer, and other ancillary services. CSCs would have to clarify with different CSPs to understand the cost structure to arrive at the overall cost of the Cloud service for comparison.

1.5 Adopting Cloud Computing Services (Identification of Needs)

1.5.1 Understanding own business needs:

- Enumerate the business needs for adopting cloud services.

1.5.1.1 Defining desired outcomes/goals:

- Define the desired outcomes, or goals CSCs want to achieve based on the identified business objectives/needs.

1.5.1.2 Nature of cloud service to acquire:

- Identify the types of cloud service and deployment models most suited to achieve the desired outcomes and business needs.

1.5.1.3 Cloud strategies (including deployment and decommissioning):

- Business strategy or ways to win customer intimacy vs product leadership vs operational excellence.
- The company's cloud strategy should be driven by its business strategy that supports business objectives/goals. Or articulate cloud strategy in terms of business strategy.
- Key service parameters (refer to MTCS self-disclosure form Annex B) should first be defined to find the best match from published CSPs' self-disclosure forms.

1.5.2 Identifying and Sourcing Potential Cloud Solutions that Meet Business Needs.

1.5.3 Cloud Considerations (once potential cloud solutions have been identified).

1.5.3.1 Cloud Risks/Challenges (shared responsibility, risk management, governance):

- Cloud security needs (refer to MTCS SS584 & Sections 2-20 in this guideline): Understand the security provisions of the CSPs and what CSCs need to do to complement to achieve the desired overall security controls.
- Outage preparedness – refer to:
  - TR 62:2018 Annex A provides indicative values for parameters of cloud outage impact categories.
  - TR 62:2018 Annex B provides a worksheet template to help capture the outage protection needs of CSCs. Refer to these two annexes to define CSCs' outage protection needs.
  - TR 62:2018 Annex C provides a template for COIR disclosure which CSPs could use to disclose their outage preparedness such as services availability,

resiliency, porting data as backup or fallback solutions in prolonged outages.
- Understand the sensitivity of data being migrated and processed in the cloud.
- Changes in IT roles and possibly business functions in the company: impact to CSCs' business and IT functions that may need to be adjusted accordingly.
- Legal and regulatory compliance: possible impact on CSCs as a result of cloud adoption.

1.5.3.2 Data Control:
- CSCs' ability to maintain control over the data being migrated/processed in the cloud
- Clarity of ownership of derived data
- Attributes of cloud usage
- Data retention period
- Data breach/loss management
- The sovereignty of data: locations of primary and backup data

1.5.3.3 Personal data protection when using cloud services
- Refer to applicable data protection guidelines (e.g. guidelines from Singapore PDPC).

1.5.3.4 Onboarding/entry and offboarding/exit:
- Understand both onboardings (what it takes to implement intended business functions including migration of related data), and,
- Offboarding (how to bring back or migrate the business functions and related data to run in another CSP) requirements to avoid a vendor lock-in situation.

1.5.3.5 Service Level Agreement (SLA) and Contractual Agreement:
- Refer to ISO/IEC 19086-3:2017 for details on various cloud SLA components that could be material to your business needs, to consider

1.6 Using the Guidelines (Selecting appropriate CSPs for the right cloud services):

Depending on the service and deployment models selected by CSCs, the boundaries between CSPs and CSCs in security responsibilities vary. Therefore, it is a shared responsibility between CSPs and CSCs for the overall success in the implementation of security for the cloud services.

The structure of this document – from section 2 onwards, it follows the requirements of MTCS SS584. It is to guide CSCs on what they should do to complement the security control provisions by CSPs. Besides security, CSCs may use the worksheet provided in Annex A to capture their business needs, other pertinent service parameters, and outage protection needs for a more comprehensive evaluation when sourcing for cloud services:

- Refer to clause 1.5.1: understand/capture business needs, use worksheet (Annex A).
- Step through clause 1.5.3 to consider and capture various cloud issues (MTCS - security, CSP self-disclosure on service parameters, outage protection) in Annex A,
- Source cloud services from CSPs with security, service parameters and outage preparedness that best meet your business, security, service, outage protection needs.
- Negotiate contractual agreement for your critical business, security, service parameters and outage protection needs and capture in the SLA.
- Jointly architect, implement and deploy the cloud solutions with CSPs.

2. Information Security Management

Guidance on implementing an Information Security Management System (ISMS) in a cloud environment. This applies to CSCs that subscribe to SaaS, PaaS, and IaaS.

a) The ISMS on cloud services could include a combination of policies, procedures, and guidelines that address the CSC's information security needs through a holistic approach, based on organisational requirements, regulatory requirements, industry practices, and other applicable standards such as ISO and NIST. The policies, procedures and guidelines relevant for cloud services should be kept up-to-date and reviewed by the CIO, CISO and cloud team lead.

b) The CSC's management (e.g. CISO, product management functions) should have policies to decide what type of data and applications can use cloud services. This includes other factors such as security, elasticity, scale and tolerance to failure that may not be available when delivering in-house IT services.

c) The CSC's management should appoint a staff member or team dedicated to handling IT security matters. The IT security member or team's roles and responsibilities should be clearly defined. The IT security team may report to the CTO directly.

d) Information security audit committees should be formally set up, and information security audit programmes should be implemented to address the information security needs for cloud services.

e) The CSC's management should provide awareness communication, conduct training for all staff and relevant parties on its ISMS. The point of contact of its information security team should be made known to all employees and appropriate parties.

3. Human Resources

Guidance for CSCs on how to implement Human Resources security for the management of cloud services. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) Background screening should be conducted before hiring personnel to manage the CSC's Cloud service. The background screening should cover at least, but not be limited to, the following:
- The applicant's Security Clearance Level (SCL) is under established standards. The SCL of the applicant should be sufficient to address the information confidentiality level.
- The applicant should have adequate experience and technical expertise in managing cloud and virtualisation environments and information security.
- Past criminal records of the applicant, if any.

b) A periodic background screening should be performed for employees granted high privilege access to the cloud system or infrastructure.

c) Background screening should also be conducted on the CSP before engaging the selected CSP. The CSC should assess the credibility and capability of the CSP to ensure that the chosen provider is qualified.

d) Information security training awareness should be conducted for staff involved in the management of cloud services. The training should be done regularly, and the content should be kept up-to-date to address the latest threats and technologies related to the cloud. The training material should be customised to make it relevant to each group of audience in the organisation and should include at least the following:
- Potential threats to cloud technology and the impact of a security breach.
- Employees' roles and responsibilities to ensure the implementation of information security in the cloud environment.
- Information security incident handling processes and procedures.

e) The CSC should ensure that access control management is in place. The access control management should create user groups with different access levels on a need-to-have basis. There should be a segregation of duty whereby the CSP cannot access the confidential information stored in the cloud network.

f) The CSC should implement strong authentication and authorisation controls for users with access to high privileges to protect the information stored on the cloud from malicious actions by employees, vendors, and CSP's employees. The controls implemented should comprise at least the following:
- Assess the necessity of implementing multi-factor authentication for accessing sensitive system resources or data.
- Assess the possibility of disabling remote access for users with access to high privileges for CSCs that subscribe to PaaS and IaaS cloud services.
- Prohibit the sharing of privileged IDs and access codes.

- CSCs that subscribe to PaaS and IaaS cloud services should also ensure that vendors and CSP's staff with privileged rights are prohibited from accessing the information stored on the cloud without any supervision or monitoring controls.

g) The employment contract should contain terms and conditions that clearly define the roles and responsibilities of the employee, including the employee's confidentiality, data protection and non-compete obligations. Notification on disciplinary actions should be clearly stated and agreed upon by the employee.

h) The CSC should implement processes to ensure that the employee's access rights to the infrastructure or system are terminated upon the employee's contract termination. This can be achieved by account deactivation/deletion/password change for sensitive systems and applications.

4. Risk Management

Guidance on how to perform risk management for the usage of cloud services. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) The board and senior management should oversee the overall risk assessment process. The risk assessment process should be performed before the development and implementation of the cloud services. The risk assessment matrix should be reviewed and approved by the CEO (or management executives) and the board.

b) The risk management framework should cover at least data protection, disaster recovery and business continuity planning in the event of unavailability of cloud services from the CSP. The risk assessment should address information security risks about cloud services such as:
- Lock-in, when the company's dependency on the CSP, data and service portability may be an issue.
- Information disclosure to the public due to failure of information isolation or other security breaches.
- Consequences of malicious actions by an employee of the CSP.
- Unavailability of the cloud service.
- Modification of the application data or information by an unauthorised user.
- Resource exhaustion: The organisation cannot provide satisfactory service to a customer due to limitations or miscalculations in the cloud service capacity.

c) The CSC should ensure that the risk register is reviewed and updated regularly to identify and address any new risk at the earliest.

d) For further guidance on information security risk management, refer to ISO/IEC 27005: 2011 Information Technology – Security Techniques – Information Security Risk Management.

5. Third Party Controls

Third-party security controls do not apply to CSCs.

6. Legal and Cmpliance

Guidance on managing the compliance requirements against applicable standards and regulatory requirements. Relevant to CSCs that subscribe to SaaS, PaaS, and IaaS services.

a) The CSC should review the CSP disclosure checklist against applicable standards and regulatory requirements and discuss the applicable audit/compliance and service level measurement criteria.

b) The CSC should ensure that the CSP performs periodic independent security assessments against the CSP's information security policies, standards and processes, as well as regulatory requirements and industry practices.

c) The CSC may request to review the CSP's dynamic compliance monitoring report, including the compliance results of system access reports, system configuration reports, and events logs.

d) The terms and conditions of cloud services with the CSP should include a list of services and support provided by the CSP and a confidential information handling agreement. The CSP disclosure checklist may be used as a guideline in composing the terms and conditions of cloud services. The contractual agreement should also state the actions and penalty clauses applicable if a security breach is caused by/performed on the CSP and their failure to comply with the SLA.

e) In the event of termination or change of CSP, CSCs whose assets are managed by the CSP should ensure that the following controls exist:

- A formal handover document is signed-off by both the CSC and the CSP. This document should also include the checklist of the assets to be handed over.
- The termination of the CSP access rights to the application data or information can be done by modifying the authentication and authorisation controls implemented, such as passwords or other authentication credential information.
- CSCs that subscribe to SaaS should ensure that the legal notice states that all data or configuration settings stored in the CSP's system are securely removed, including the backup data.

7. Incident Management

Guidance on how to develop the incident management framework for cloud services. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) The CSC should develop an incident management framework for cloud services. A policy may be developed as part of the framework. The policy should state the roles and responsibilities of each CSC and the roles and responsibilities of the CSP management in the incident handling process.

b) The incident management framework should also include the incident handling procedures, which describe in the minimum, the following essential information:
- Immediate steps to be taken in countering an attack.
- Escalation procedures.
- Resolution timeframe.
- Activation of service continuity arrangements.
- Trigger of alerts.
- Report generation.
- Methods to inform the affected personnel or the customer.

c) The management should conduct incident response awareness training to educate all employees or team members on the incident response process, procedures and the reporting schema.

d) The CSC should ensure that the CSP assigns a point of contact or a reporting centre for incident reporting and other information security issues.

e) A list of contacts for an incident response should be distributed to all staff in the company and the CSP. The contact list should also include the personnel from CSP who the information security personnel can reach in an incident.

f) The incident management framework of cloud computing services may be built based on the CSC's incident management framework. The same reporting centre may be utilised, and the same root cause analysis method may be used.

g) It is also recommended that the customer retain evidence of the incidents to aid future investigations and analysis.

h) The CSC should develop a mechanism to track the list of incidents and the follow-up status of each item in the list. A periodic review of the incident management process and procedures should be performed.

i) The outcome of the incident management process where data is collected may be used for subsequent problem management processes. The review can be performed by collecting evidence and analysing the list of incidences over time.

j) For additional details, please refer to the following reference: http://www.sans.org/reading_room/whitepapers/incident/incidents-Cloud_33619

8. Data Governance

Guidance on how to develop a data governance framework for cloud services. This guideline applies to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) CSCs should establish a data governance framework (i.e. data classification, secure handling, secure disposal) for confidential information stored on the cloud.

b) The SLA between the CSC and CSP should include confidentiality and non-disclosure provisions. The confidentiality clause should include data confidentiality protection provisions that require all CSC data to be safely/securely removed from the respective CSP when the service is terminated.

9. Audit Logging and Monitoring

Guidance on how to manage audit logging and monitoring for cloud services. This guideline applies to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) CSPs may provide a report of the log review regularly, such as weekly or monthly. The CSC should ensure that the report covers configurations deemed essential to the CSC and related to the services subscribed, such as system faults, system performance, backup process status, or intrusion detection.

b) The management should sign off the log review report provided by the CSP. Additionally, a reasonable log retention period should be set.

10. Secure Configuration

Guidelines for the CSC to implement cloud services are securely configured. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) CSCs should ensure that the systems and applications hosted in the cloud are securely configured based on regulatory requirements and industry practices. The CSC may work with the CSP to arrange for the required security controls or resources to be provided by enhancing the authentication and authorisation controls to the system, such as strong passwords, using non-default accounts and passwords, access controls, patch management, etc. For details, check: Center for Internet Security Division: http://benchmarks.cisecurity.org/en-us/?route=downloads.benchmarks

b) CSCs should ensure that each user who accesses the application must be authenticated and authorised before accessing the sensitive data.

11. Security Testing and Monitoring

The following guide security testing and monitoring. This guideline applies to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) For CSCs who subscribe to SaaS cloud services, an agreement with the CSP should be made for security assessments (e.g. penetration testing) to be conducted.

b) For CSCs that subscribes to IaaS and PaaS, periodic security assessments should be conducted for the systems hosted in the cloud.

c) The CSP should provide a suitable environment for security testing.

12. System Acquisition and Development

The following guide system acquisition and development. This guideline applies to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) CSCs developing their applications should ensure that a system development lifecycle framework is followed for applications developed in the cloud.

b) The information security team should conduct periodic threat and vulnerability assessments and ensure that the cloud services meet their security requirements.

c) The CSP should provide a suitable test environment for CSCs to determine if the development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities has common vulnerabilities. This can be performed by verifying the cloud service against industry standards: Open Web Application, Security Project (OWASP) Top 10, SANS Top 25 and Software Assurance Forum for Excellence in Code (SAFECode).

13. Encryption

Guidance on how to implement encryption controls about the system and services hosted in the cloud. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS services.

a) CSCs should ensure that confidential data such as the user's password or credit card number is encrypted before storing such data on the cloud. The encrypted data can be a file, a disk or an entire virtual machine. The encryption key should be handled by the CSC or end-user instead of the CSP.

b) Confidential data should not be transmitted in clear text to the server. At a minimum, communication channel encryption should be implemented in the data transmission from the end-user to the server.

c) Robust encryption methods and cryptography controls should be implemented as per prevailing industry standards.

14. Physical and Environmental Security

Physical and environmental security controls are not applicable for SaaS and PaaS CSCs.

a) For IaaS, refer to the guidelines for CSPs.

b) In addition, CSCs should ensure the following: CSC networks, systems, endpoint, and physical security are commensurate with the degree of data confidentiality, integrity, and availability required.

15. Operations

Guidance on how to develop operational controls in the system and services hosted in the cloud. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) Cloud services operations policy and procedures documentation should be developed. The process and procedure documents should include at least the following:

- Roles and responsibilities of the CSC's cloud service management team.
- Functions and duties of the CSP.
- Process of granting, modifying or revoking of user access controls as well as handover processes when the CSP is changed.
- List of critical systems or data to be monitored by the CSC's cloud service management team. The monitoring process can be used as per methods for information security breach detection.
- Procedures of business continuity planning and incident response to be handled if the CSP is not available.

b) The CSP and the CSC should have clear documentation on the agreed SLAs provided.

16. Change Management

Guidance on change management of systems and services hosted in the cloud. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) The CSC should ensure that the CSP has a formal change management process to manage cloud services.

b) The SLA between the CSC and the CSP should also include the retrieval of backup data. The backup retention period should be made known to the CSC, and the CSP should be able to provide the backup data upon customer request.

17. Business Continuity Planning and Disaster Recovery

Guidance on implementing business continuity planning (BCP) and disaster recovery (DR) about the systems and services hosted in the cloud.

a) Risk assessment should be performed to identify systems or data which require BCP and DR contingency plans.

b) If information and systems hosted on the cloud are mission-critical, the CSC should assess whether the cloud service subscribed caters to BCP and DR.

c) Before engaging the CSP, the CSC may assess the sufficiency of BCP and DR services provided. The CSC may request that the DR site be hosted at a different data centre or location.

d) The CSC may engage another CSP as a backup vendor as part of the BCP.

18. Cloud Services Administration

As additional references, the following could be referred for details on segregation of duties:

a) "An Overview of Sarbanes-Oxley for the Information Security Professional": http://www.sans.org/reading_room/whitepapers/legal/overview-sarbanes-oxley-information-security-professional_1426

b) "Separation of Duties in Information Technology": http://www.sans.edu/research/security-laboratory/article/it-separation-duties

19. Cloud Services Customer Access

Guidance on how to control user access to the system and services hosted in the cloud. Applicable to CSCs that subscribe to SaaS, PaaS, and IaaS cloud services.

a) CSCs who subscribe to IaaS and PaaS cloud services should ensure that a user access matrix is created and user access rights to the infrastructure and backend system are granted according to the user access matrix defined.

b) CSCs that subscribe to SaaS cloud services should assess and review the requirement of a group of users according to their user roles. When a user role is implemented, the CSP should authenticate and restrict user access according to the function defined.

20. Tenancy and Customer Isolation

No additional guidance.

Annex A – A Checklist of Business Needs & Cloud Considerations

S/No	Business Needs / Cloud Considerations	Level of Importance	Desired Outcomes

Annex B – Cloud Service Provider Disclosure

From Annex A of MTCS SS584:2020:
The form is to be completed for each cloud service provided. For questions not applicable or not disclosed, indicate accordingly in the remarks.

Date of Disclosure:
Applicable cloud service/s:

CSP Contact Information
Company name: Primary address: Web address: Contact name: Contact number: Contact email: MTCS Certificate Number: Company Chop Company Representative Signature:
Certification Body Contact Information
Company name: Web address: Contact name: Contact number: Contact email: Company Chop: Lead Auditor Signature:
CSP Background
Overview of service offering:

Service model:

☐ VM instances owned by the CSC.

☐ 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 CSC has the right to audit: ☐ VM instances owned by the CSC. ☐ Network facilities. ☐ Compliance with applicable standards. ☐ Technical controls. ☐ Policies and governance. ☐ Data centre facilities. ☐ Others. ☐ None.	

No	Criteria	Description	Remarks
		Regulators under Singapore law have the right to audit: ☐ VM instances owned by the CSC. ☐ Network facilities. ☐ Compliance with applicable standards. ☐ Technical controls. ☐ Policies and governance. ☐ Data centre facilities. ☐ Others. ☐ None. Audit/assessment reports to 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	Following guidelines/standards/regulations are adhered to: ☐ Singapore Personal Data Protection Act. ☐ ISO / IEC 27001. ☐ ISO 9000. ☐ ISO / IEC 20000. ☐ CSA Open Certification Framework.	

No	Criteria	Description	Remarks
		☐ PCI-DSS. ☐ Others	
Data Control			
3.	Data Ownership	All data on the cloud service is owned by the CSC, except: The CSC retains ownership of the derived data or attributes of cloud usage except for the following: ☐ Advertising or marketing. ☐ Statistics analysis on use. ☐ Others.	
4.	Data Retention	Data deleted by the CSC is retained as follows: ☐ The minimum data retention period is: ☐ The maximum data retention period is: ☐ Deleted immediately. Log data is retained for a period of: ☐ The minimum data retention period is: ☐ The maximum data retention period is: ☐ Not retained. CSC data is retained for a period of: ☐ The minimum data retention period is: ☐ The maximum data retention period is: ☐ Not retained. Following types of data available for download by the CSC: ☐ Log data.	

No	Criteria	Description	Remarks
		☐ Others:	
5.	Data Sovereignty	The primary data locations are: ☐ Singapore. ☐ Asia Pacific: ☐ Europe: ☐ United States: ☐ Others: The backup data locations are in: ☐ Singapore. ☐ Asia Pacific: ☐ Europe: ☐ United States. ☐ Others: No. of countries in which data centres are operated: The CSC'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 stated: ☐ No. CSC's consent is required before transferring data to a location not specified in item 5 or a third party: ☐ Yes. ☐ Yes, except as required by law. ☐ Yes, except as stated: ☐ No. *Note: CSCs are responsible for determining the impact of data protection and data sovereignty laws on the locations where data is stored. CSCs should understand the risks associated with relevant laws that may allow government access to data-in-transit or storage with CSPs.*	

No	Criteria	Description	Remarks
6.	Non-Disclosure	☐ CSP can provide an NDA template. ☐ CSP may use the customer's NDA (after legal review).	
Provider Performance			
7.	Availability	The committed network uptime is: _____ % ☐ Varies according to the price plan. The committed system uptime is: _____ % ☐ Varies according to the price plan. The cloud environment has these single points of failure: ☐ Please specify: ☐ None.	
8.	3rd party Dependency	Highlight areas of critical dependency for service delivery:	
9.	BCP / DR	☐ Disaster recovery protection. ☐ Backup and restore service. ☐ CSC selectable backup plans. ☐ Escrow arrangements. ☐ No BCP / DR is available ☐ RPO: ☐ RTO: ☐ Others, please specify:	
10.	Liability	The following terms are available for the CSC on the failure of the provider to meet the SLA commitment: ☐ Network failure. Liability:	

No	Criteria	Description	Remarks
		☐ Infrastructure failure Liability: ☐ VM instance failure Liability: ☐ Migrations Liability: ☐ Unscheduled downtime Liability: ☐ Database failure Liability: ☐ Monitoring failure Liability:	
11.	Shared Responsi-bility	☐ Communication of shared roles & responsibilities for which CSC needs to implement and manage for the use of this cloud service URL (or attach file):	
Service Support			
12.	Change Manage-ment	The CSP 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 older versions for a defined period. ☐ Ability to choose the timing of the impact.	

No	Criteria	Description	Remarks
13.	Self-Service Provision-ing & Manage-ment Portal	Provide self-service provisioning and management portal for CSCs 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, network) and service templates. ☐ Track and manage the lifecycle of each service. ☐ Track consumption of services. ☐ Health monitoring. ☐ Others:	
14.	Incident & Problem Manage-ment	The delivery mode of support: ☐ Access via email. ☐ Access via a portal. ☐ Access via phone support. ☐ Direct access to support engineers. Availability of support: ☐ 24 x 7. ☐ Office hours support, specify the hours of operations: ☐ After-office hours support, specify operation hours: Service response time: Notification time of cloud service outage incident:	

No	Criteria	Description	Remarks
		Communication channel used for notification of cloud service outage incident: The following are available to CSCs upon request: ☐ Permanent access to audit records of customer instances. ☐ Incident management assistance. Incident response time: Mean time to repair on detection of faults:	
15.	Billing	The following billing modes are available (please elaborate granularity of charges and measurement): ☐ Pay per use: ___ (up to per min/hour/day/month for compute/storage for IaaS/PaaS, and per CSC per hour/day/month/year for SaaS) ☐ Fixed pricing_____(up to yearly/monthly/daily) ☐ Other pricing models: ☐ Not disclosed/ ☐ Available billing history: ____ Months	
16.	Data Portability	Importable VM formats: Downloadable formats: JSON/XML/other open formats: Supported operating systems: Language versions of supported operating systems: Supported database formats: Policy/guide available: API: ☐ Common. ☐ Customised.	

No	Criteria	Description	Remarks
		Upon service termination or prolonged outage, data is available through: ☐ Physical media. ☐ Standard methods as described above. ☐ Other methods	
17.	Inter-Operability	Use of industry standards and availability of APIs to support interoperability: ☐Transport supported (e.g. REST-based HTTPS/MQTT): ☐ Format supported (e.g. JSON/XML): ☐ APIs supported: ☐ Other methods: Guide available:	
18.	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:	
19.	User Manage-ment	☐ Identity management. ☐ Role-based access control. ☐ Federated access model. ☐ Integration with Identity management solutions. ☐ Others:	
20.	Lifecycle	The CSC may select the following for service upgrades and changes:	

No	Criteria	Description	Remarks
		☐ Automatic provisioning. ☐ CSC customisable provisioning.	
Security Configurations			
21.	Security Config-uration Enforce-ment 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?	
22.	Multi-Tenancy	☐ Distinct physical hosts. ☐ Separate physical network infrastructure. ☐ Virtual instance grouping. ☐ CSC definable security domain. ☐ CSC customisable firewall. ☐ CSC definable access policies.	
23.	Hybrid Cloud Provision	Ability to monitor, track, apply and enforce CSC's security & privacy policies on its cloud workloads: ☐ Data protection and encryption key management enforcement geolocation-based/resource pools and secure migration of cloud workloads. ☐ Key management and Keystore controlled by CSC. ☐ Persistent data flow segmentation before and after geolocation-based/resource pools secure migration. ☐ Compliance enforcement for regulated workloads between on-premises private and hybrid/public cloud. ☐ Others:	
Service Elasticity			

No	Criteria	Description	Remarks
24.	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 unusually 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):	
25.	Network Resiliency & Elasticity	Following network resiliency/elasticity options are available: ☐ Redundant Internet connectivity links. ☐ Redundant Internal connectivity. ☐ Selectable bandwidth up to ___ 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: ☐ Shared or dedicated bandwidth, please specify: ☐ QoS traffic control services. ☐ Alerts to be sent for unusually high usage. ☐ The minimum performance during peak periods: ☐ The minimum period to scale up network throughput:	

No	Criteria	Description	Remarks
26.	Storage Redundancy & Elasticity	Following storage redundancy/elasticity options available: ☐ Redundant storage connectivity links in each data centre: ☐ Redundant storage connectivity links between DCs belonging to the same cloud: ☐ Storage traffic isolation, please specify: ☐ Shared or dedicated storage network bandwidth: ☐ Quality of service for storage traffic control services: ☐ Maximum storage capacity for the entire cloud: ☐ Maximum storage capacity for single CSC: ☐ Maximum expandable storage, please specify: ☐ Alerts to be sent for unusually high usage. ☐ Minimum storage I/O performance during peak periods: ☐ The minimum period to scale up storage I/O throughput:	

Annex C – Template for COIR Disclosure Form

Annexe C of COIR TR62:2018: This template illustrates how CSPs can use COIR protection parameters to share their capabilities to manage outages of the subscribed cloud service.

A. Company information			
Company name: Primary address: Web address: Contact number: Contact name, designation: Contact email: Company stamp: Signature of company representative:			
Date of disclosure:			
B. Applicable Cloud services			
Service description:			
Type of service (tick √ where appropriate): ☐ IaaS ☐ PaaS ☐ SaaS ☐ Others			
No	**Parameter**	**"As-is" COIR practice**	**Remarks**
1	Service availability		
2	Historical availability record		
3	Recovery time objective		
4	Recovery point objective)		
5	Support hours		
6a	Notification channel of planned maintenance		
6b	Notification lead time of planned maintenance		
7	Frequency of health monitoring of cloud service		
8	Health monitoring mechanisms for use by CSC		
9	Sharing of COIR plan		
10	Exercise of COIR plan		
11	Notification time of cloud outage incident		
12	Communication channels used for notification of cloud outage incident		

13	Communication channels for CSC to report cloud outage		
14	Response time by CSP		
15	Frequency of status update of the reported outage		
16	Communication channels used for status updates		

Notes:

1. CSPs may choose to identify the closest COIR category for each service disclosed to disclose their existing operating COIR practices for each parameter.
2. CSPs are not expected to change their current outage protection practices to meet the indicative value of the categories for the parameters.
3. CSPs can highlight any derivations from the category's indicative value of the parameters in the remarks column.
4. The differences could include better values than the indicative or multiple values associated with different costs.
5. CSPs may refer to similar past/exemplary implementations for bespoke cloud services to declare the COIR parameters.