

## **1.0 PURPOSE**

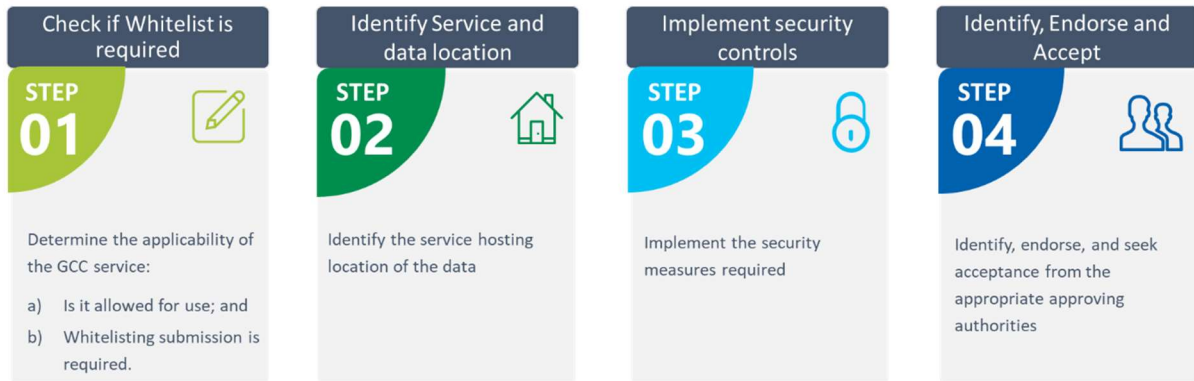
This document serves as a guideline for Agencies' to determine if a GCC native service will require a Whitelisting submission prior to its use.

## **2.0 GETTING STARTED – Overview of the Guidelines**

Agency will be required to undergo a four-step process to identify if a whitelisting submission is required for the use of a GCC native service.

**Guidelines for identification of hosting location for GCC native service**

The below steps provides Agencies' with the guidelines for identifying the hosting location of the cloud native service and also the steps required prior to the use of overseas cloud native service.




**Step 1 – (1/4) Check to confirm if the CSP service is exempted from whitelisting**

Agencies are first required to identify if the CSP service is allowed for use and if a Whitelisting submission is required.

To be exempted from the Whitelisting request, Agencies are required **meet the two conditions** below.

Use of Predefined Markers	
Markers	Definition of IaaS, PaaS
1	<p>Provided by any of the three CSPs</p> <ul style="list-style-type: none"><li>• Google Cloud</li><li>• Amazon AWS</li><li>• Microsoft Azure</li></ul> <p>And made available through GCC only</p>
2	<p>Supports the delivery and operational aspects of the Agency system</p> <p><i>This is to limit only for those services that are directly used to support the delivery or operationalization of Agency-deployed systems, such as AWS Guard Duty, Azure Security Center, Google Cloud Logging etc.</i></p>



Yes/No

Examples			
M365	D365	AWS Chime	Workday
No, it is not made available through GCC		Yes	No, it is not made available through GCC
No, it is used directly as an application.			
All systems and infrastructure platform, and security of the data are managed directly by the vendor where consumers would not have control over.			

## Step 2 – (2/4) - Agency to identify the GCC Service and data hosting location



For Step 2, Agencies' are required to:

- 1) Identify the hosting location of the GCC native service; and
- 2) Store Primary data in Singapore.

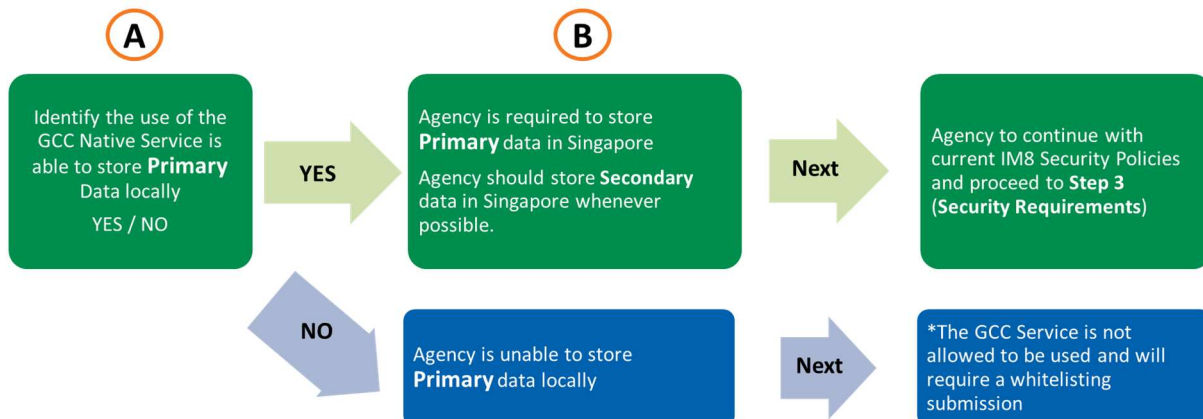
For GCC native services with *Primary* data stored out of Singapore, Agencies' are required to submit a Whitelisting request and seek CSG's approval prior to use.

### Prioritisation of Data in the Cloud

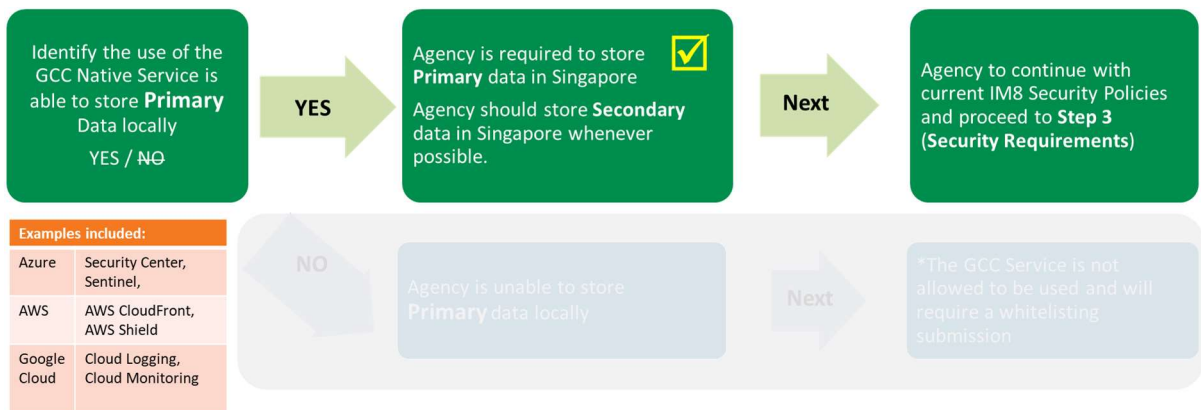
Category	No	Type of data used by GCC service	Description	Examples	Requirements
Primary	1	Business	Core data of a system that provides the most value to and is most often used by Agencies	<ul style="list-style-type: none"> <li>Database storage, such as block, file and disk</li> <li>Project related data, such as architectural diagram and business logic</li> </ul>	Agencies' are <b>required</b> to store the data locally
	2	Security	Data that is used to manage the security of a system	<ul style="list-style-type: none"> <li>System accounts</li> <li>Credentials storage</li> <li>Keys (private)</li> <li>PKI Certificates</li> </ul>	
Secondary	3	*Coding	Project related source code repositories	<ul style="list-style-type: none"> <li>Programming languages, such as Python, Java, Java script, PHP, Ruby, C# and C++</li> </ul>	Agencies' <b>shall store the data in Singapore</b> as the default option where possible. Agencies shall only consider the storage of data outside of Singapore if there are no available options and after conducting a risk assessment.
	4	Compliance	Data of a system that is used for compliance purposes, such as event logs	<ul style="list-style-type: none"> <li>Security logs</li> <li>Audit logs</li> <li>Application logs</li> </ul>	
	5	Configuration	Data is used to describe the configuration of a system	<ul style="list-style-type: none"> <li>Operating system hostnames</li> <li>IP addresses, subnet mask, ports and protocols</li> <li>Metadata of file, such as type, size and last modified</li> </ul>	
	6	Public Accessible data	Data that is meant for the public's consumption or openly sourced from the Internet	<ul style="list-style-type: none"> <li>Content from publicly available Internet websites, such as HTML scripts, news reports and images</li> </ul>	

*\*If the Agency assesses that the unauthorised disclosure of the source code will result in an impact to the Agency, the source code should be re-classified to the Primary category*

### Flowchart



*\*Agency should write in to [CSG\\_Cloud\\_Service\\_Whitelisting@tech.gov.sg](mailto:CSG_Cloud_Service_Whitelisting@tech.gov.sg) to seek clarifications if needed.*

**Example**

**Step 3 – (3/4) - Agency to implement security controls**

The Cloud Security Model (CSM) is used to draw up the security requirements for the secure deployment of Agencies' RESTRICTED systems and data when using overseas GCC native services.

The security measures are identified based on the required controls for securing the data throughout its lifecycle.

Cloud Security Model	
Domain	Purpose
Visibility	Securing your asset is knowing exactly what and where they are <ul style="list-style-type: none"> <li>Ensuring that Agencies are aware of the details of where their secure data is hosted</li> </ul>
Protection	Provision of security full stack implementation and continuous monitoring <ul style="list-style-type: none"> <li>Ensuring that the Agencies' data is secure throughout its lifecycle</li> </ul>
Auditability	Ability to verify and validate the effectiveness of protective measures <ul style="list-style-type: none"> <li>Ensuring that Agencies' users' privileged and administrative activities are closely monitored for any unauthorised or malicious activities.</li> </ul>

**Security requirements for use of GCC managed overseas cloud native services**

Instructions:		Agency to understand and meet each security requirements	Agency to use suggested methods or other possible means to achieve each security requirement				Agency's use	
CSM Domains	No.	Security Requirements to protect data	Suggested Methods	AWS	Azure	Google	Checkbox	Comments (if any)
Visibility	1	Ensure that all the application business data in the cloud's storage are residing in Singapore.	Agency should store the data in Singapore as the default option where possible. Agency should only consider the storage of data out of Singapore if there are no available options available and after conducting a risk assessment.	Virtual Instances Block Storage (S3) Disk Storage (EBS) Database (RDS, SQL) Containers (EKS, ECS) ECR (Elastic Container Registry)	Virtual Machine Disk Storage Blob Storage Database (SQL, MySQL) Container Instance Container Registry	Compute Engine Persistent Disk Cloud Storage Cloud SQL Cloud Bigtable Container Engine Container Registry	<input type="checkbox"/>	
	2	Ensure that Key Management Systems are minimally certified FIPS 140-2 Level 2.	Agency should use key management services provided by GCC native service or dedicated HSMs which meets the FIPS 140-2 Level 2 certification.	KMS Secrets Manager Cloud HSM	Key Vault Cloud HSM	GCP KMS	<input type="checkbox"/>	
	3	Ensure cryptographic keys are rotated regularly, such as every six months or 12 months.	Agency should use key management services provided by GCC native service or dedicated HSMs to perform key rotation. The cryptographic keys should be rotated based				<input type="checkbox"/>	

			on a frequency defined by the Agency.					
	4	Ensure that all the accounts that are granted with the permission to manage and administrate the keys are reviewed based on IM8's requirement, and remove all excessive permissions.	Agency should perform a review of user accounts that are administrating key management services/systems and remove excessive permission. The frequency of the account review should be based on IM8 Application Development Security #2.3/S6.				<input type="checkbox"/>	
	5	Ensure that processes are established for management of cryptographic keys, such as key lifecycle, key allocations and key rotation.	Agency should document changes to cryptographic key policies, such as creation, assignment, disable and deletion of cryptographic keys.				<input type="checkbox"/>	
Protection	6	Ensure that data-at-rest is encrypted, such as block, file, directory and snapshot level.	Agency should use GCC native services or third party encryption tools for securing data-at-rest.	Block Storage Encryption Volume Encryption File Encryption Database Encryption			<input type="checkbox"/>	



	7	Ensure that data in-transit is encrypted over untrusted networks.	Agency should use encrypted channels and protocols for communications performed over the Internet or any other untrusted networks, such as HTTPS, SSL, IPSec and SFTP. The use of encrypted channels and protocols should be based on IM8 Application Development Security #3.1.	Load Balancer Certificate manager	App Gateway	Cloud Load Balancing	<input type="checkbox"/>	
	8	Identify all possible data flows and critical path.	Agency should document the data communication channels, such as TCP traffic, API calls, Intranet/Internet Compartments and Security Groups, that has been created for the different compartments.	Trusted Advisor Security Hub	Security Centre	Command Centre	<input type="checkbox"/>	
	9	Ensure that the data are segregated according to Agency's requirements and environment	Agency should segregate the data between the different environments, such as production, non-production, User Acceptance Testing (UAT), development and operating environments.	VPC Compartment (Intranet/Internet/Management Zone)	VNET Compartment (Intranet/Internet/Management Zone)	VPC Compartment (Intranet/Internet/Management Zone)	<input type="checkbox"/>	
Auditability	10	Ensure that data access is based on Principle of Least Privilege (PoLP), such as pre-defined roles, customised or attribute roles.	Agency should create and assign pre-defined roles to user and security groups. For internal communication between GCC native services,	IAM policies Resource level policies Organization level policies			<input type="checkbox"/>	

			Service Accounts should be used.					
	11	Ensure personnel with access to data are security cleared.	Agency should subject project personnel to the require level of security clearance, such as CAT2.	Not Applicable			<input type="checkbox"/>	
	12	Ensure that user access rights are regularly review, such as role, groups and policies.	Agency should conduct reviews of: - User accounts and access rights based on the frequency defined in IM8 Application Development Security #2.3/S6; and - CASB security alerts of user accounts and access rights.	Trusted Advisor	Security Centre	Command Centre	<input type="checkbox"/>	
	13	Ensure that privileged accounts are closely monitored for any unauthorized or malicious activities that may occurred.	Agency should use CSP services to trigger alerts, such as e-mail notifications, on malicious activities performed by privileged accounts.	Configure auto backup retention and deletion settings	Log Analytics Event Hub Security Centre	Stack Driver Logging Cloud Security Command Centre	<input type="checkbox"/>	
	14	Ensure that alerts are trigger for changes in user access rights.	Agency should use CSP services to trigger alerts, such as e-mail notifications, for changes to user access rights, such as				<input type="checkbox"/>	

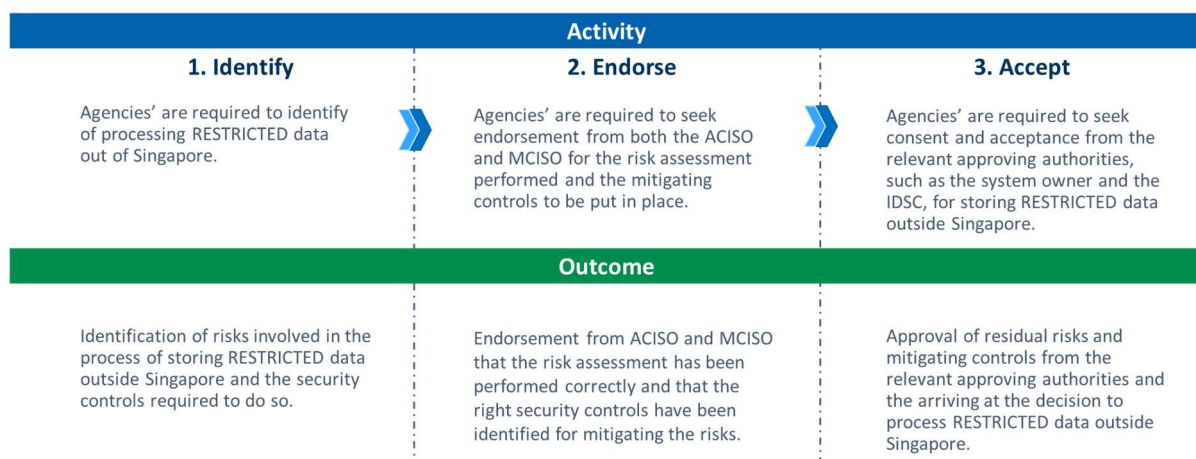
			creation, deletion and modification.					
	15	Ensure that the lifecycle of the data is managed in accordance with the Agency's requirements.	Agency should manage and store data in accordance with the Agency's project timeline and requirements.	Use of GCC native service policies to define: - Geographic hosting location of the data; and - Conditions for the transfer and archival of data.			<input type="checkbox"/>	
	16	Ensure that data is securely deleted when it has reached the end of its lifecycle in Agency.	Agency should delete both the encrypted data and their corresponding encryption keys, when the data is no longer required.	Configure auto backup retention and deletion settings			<input type="checkbox"/>	
	17	Ensure that the data is backup and restored in accordance with the Agency's requirements.	Agency should develop the backup and restore strategies and test these strategies based on a frequency defined by the Agency.	Configure auto backup retention and deletion settings			<input type="checkbox"/>	

## Step 4 – (4/4) - Agency to identify, seek endorsement and acceptance from the approving authority of the residual risk



Agencies are required to identify, endorse, and seek acceptance from the relevant approving authorities on the storage of RESTRICTED data out of Singapore.

The diagram below provides the required activities to follow and outcomes to achieve.



The below table describes the roles and responsibilities that stakeholders should be undertaking in the process.

Steps	Activity	Description	Project Team	ISM/CIO	A-CISO	M-CISO
Step 1	Check if Whitelist is required	Determine the applicability of the GCC service: a) Allowed for use; and b) Whitelisting submission is required.	R	A	C	I
Step 2	Identify Service and data location	Identify Global GCC Service for use and the hosting location	R	A	C	I
Step 3	Implement security controls	Implement the security measures required for use of Global GCC service and cloud services available to meet security requirements	R	A	C	I
Step 4	Identify, Endorse and Accept	Identify, endorse and seek acceptance from the authorized approving authorities on the hosting of classified data overseas	~Risk acceptance approving authority is dependent based on residual risk level.		C	I

R – Responsible | A – Accountable | C – Consulted | I – Informed

~ Risk Acceptance approving authority, <https://intranet.mof.gov.sg/portal/IM/Themes/IT-Management/Set-policies,-standards-and-guidelines-for-ICT-man/Topic/Risk-Management.aspx>

\*Responsibility Assignment Matrix (RACI) Model, Responsible/Accountable/Consulted/Informed <https://www.projectmanagement.com/wikis/234008/RACI>

**Approving authorities of residual risk**

	Risk to systems owned by a statutory Board	Risk to systems owned by a ministry	Risk to SGNet and Whole-of-Government <sup>1</sup>	Risk to systems owned by an Organs-of-State
Very High	Cannot be accepted <sup>2</sup>			
High <sup>3</sup>	Chairman of board	PS of Ministry or equivalent	PS SNDG	Head of Agency, or equivalent
Medium-High	Head of Agency or equivalent	Chairperson of IDSC, Head of Agency, or equivalent	CE GovTech	
Medium	Chairperson of IDSC, or equivalent	Chairperson of IDSC, or equivalent	Chairperson of GovTech IDSC, or equivalent	Chairperson of IDSC, or equivalent
Low	Chairperson of Project Management Committee, or CIO			
<sup>1</sup> If the risk may potentially impact SGNet and Whole-of-Government, risk acceptance from individuals in this column will apply in conjunction with the other relevant columns				
<sup>2</sup> In times of national emergencies, guidance from existing legislations would be used for the treatment and acceptance of risks				
<sup>3</sup> Recommended not to accept this risk level, and to reduce the risk level				