



# Understanding NUS Cloud Policy and Cloud Assessment

## Overview of NUS Cloud Policy

- Governs the use of cloud in the University
- Aims to ensure secure, compliant, and well-managed cloud usage
- Applies to all NUS staff using cloud to process University Data

## Understanding Cloud Assessment

- Business, data and technical risks must be evaluated before using any cloud
- Assessment involves evaluating the technical aspects and security of the cloud, as well as ensuring compliance with personal data protection requirements

## When to Submit Cloud Assessment

- A cloud assessment must be submitted and approved **PRIOR TO** the use of any cloud
- Re-assessment of an assessed cloud is required if:
  - Data sensitivity increases
  - There are significant changes in service scope and provider terms
  - For critical services: every 2 years

## How to Submit Cloud Assessment

- Cloud assessment or re-assessment request can be submitted at:  
<https://nusit.nus.edu.sg/cloud-assessment/CloudAssess>
- Both assessment and re-assessment follow the same review process

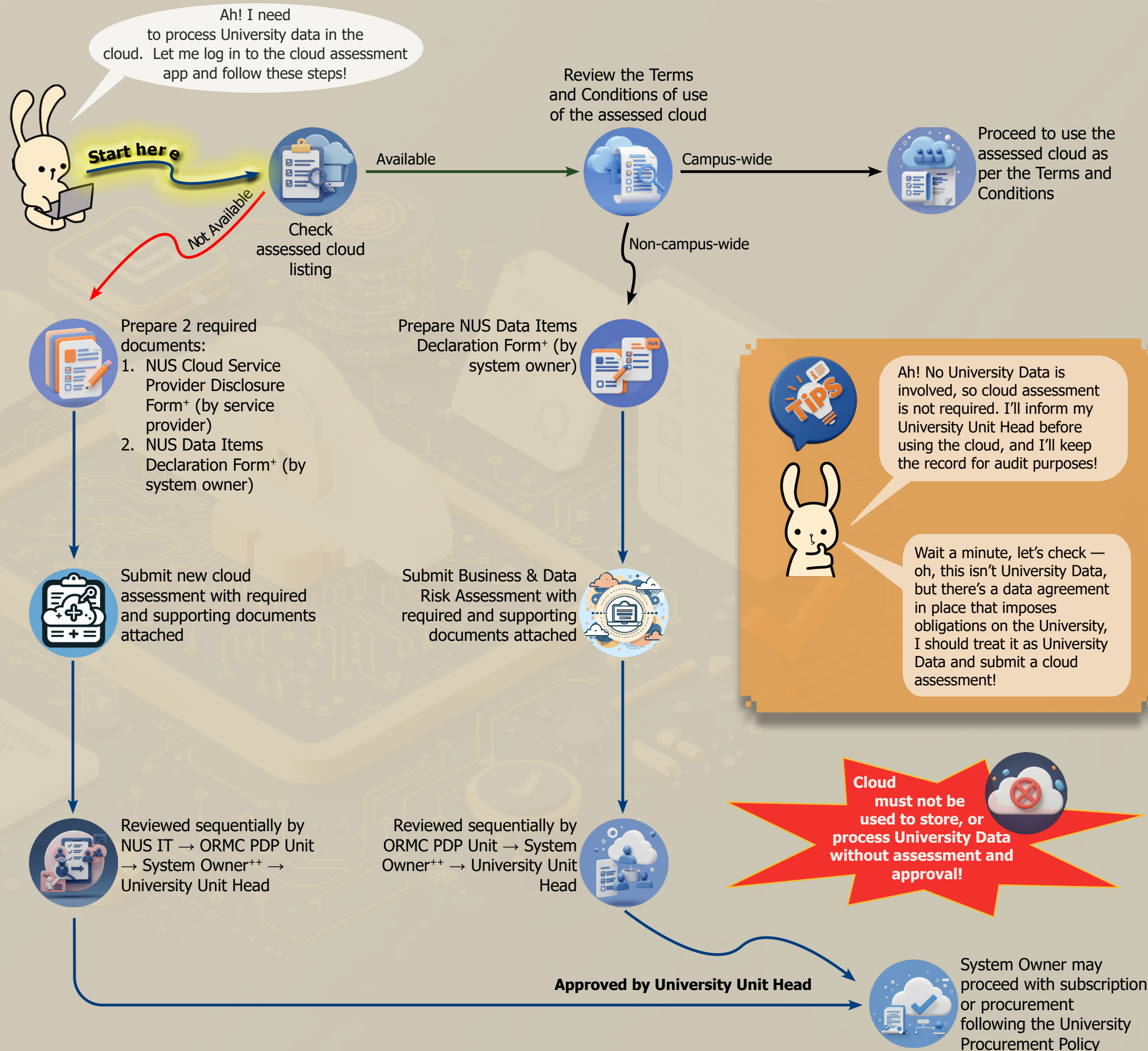
I need more information

**NUS Cloud Policy, NUS DMP & other NUS Policies:**  
<https://nusu.sharepoint.com/sites/ormc/NUSpolicy/SitePages/policies-guidelines-policyname.aspx>

**NUS Cloud Assessment Portal:**  
<https://nusit.nus.edu.sg/cloud-assessment>

**NUS Cloud Policy Contact:**  
[NUSCloudPolicy@nus.edu.sg](mailto:NUSCloudPolicy@nus.edu.sg)

## Next Step: Submitting Your Cloud Assessment



<sup>+</sup> Latest form templates are available for download in the Cloud Assessment App

<sup>++</sup> System Owner should consult OLA if there are concerns regarding the service provider agreements





# Cloud Security Responsibilites and Guidance

## System Owner’s Checklist

-  **Secure Cloud operation**  
follow NUS IT Security Policy, NUS Data Management Policy, and Data Protection Policy and Procedures.
-  **Authenticate and authorise Cloud users**  
follow NUS IT Security Policy: Chapter 4 Access Control Security
-  **Manage Cloud security**  
include patching, configuration, and monitoring
-  **Cloud administration guide<sup>+</sup>**  
prepare, maintain and review the roles, and responsibilities of System Owner, users, and Cloud provider

+ Optional if the cloud model is Software as a Service and it is not critical to project success.

## Cloud Security Responsibilities

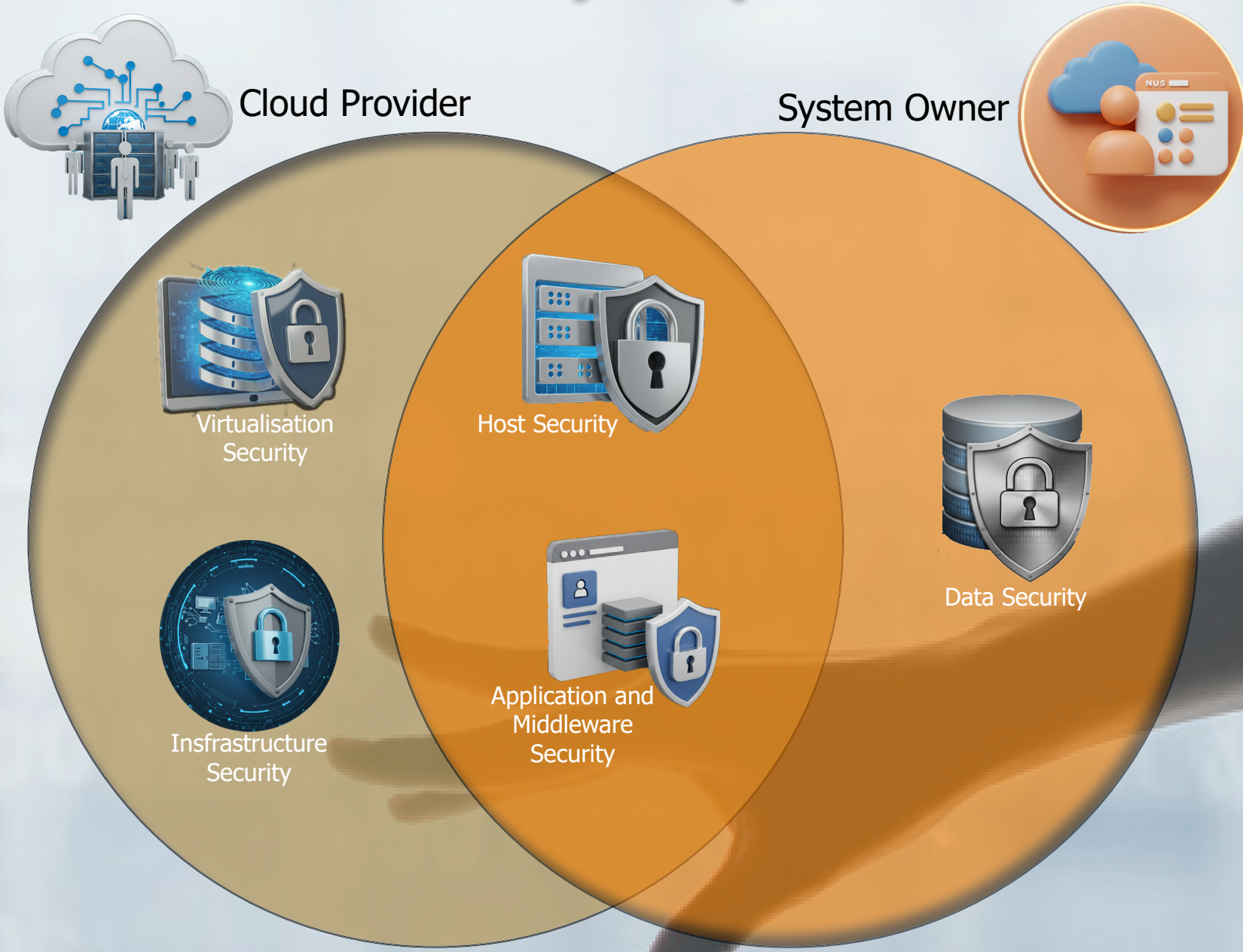



TABLE: CLOUD SECURITY RESPONSIBILITIES BY CLOUD MODEL (Reference: <a href="https://cloudsecurityalliance.org/artifacts/guideline-on-effectively-managing-security-service-in-the-cloud/">https://cloudsecurityalliance.org/artifacts/guideline-on-effectively-managing-security-service-in-the-cloud/</a> )				
Security Type \ Cloud Model	Infrastructure as a Service	Platform as a Service	Software as a Service	
Data Security	System Owner	System Owner	System Owner	
Application Security	System Owner	System Owner	Cloud Provider	
Middleware Security	System Owner	Cloud Provider	Cloud Provider	
Host Security	System Owner	Cloud Provider	Cloud Provider	
Virtualisation Security	Cloud Provider	Cloud Provider	Cloud Provider	
Infrastructure Security	Cloud Provider	Cloud Provider	Cloud Provider	



### Guidance for System Owner

#### Preparing the Cloud Administration Guide

1

Roles & Responsibilities

- Define Cloud provider responsibilities
- Define System Owner responsibilities for IaaS or PaaS (e.g., appoint application administrator and/or system administrator)

2

User & Admin Access

- Process for granting, modifying, or revoking users
- Process for granting, or revoking administrative privileges

3

Configuration & Security Procedures

- Modifying configuration settings
- Vulnerability scanning
- Applying patches for vulnerabilities
- Maintaining other cloud security settings

4

PaaS Application Security Requirements

- Vulnerability scanning
- Identity and access management
- Application firewall
- Other application security measures

5

IaaS Infrastructure Security Requirements

- Antivirus, server hardening, patch management
- Database and API security
- Application security requirements (see 4 above)
- Other infrastructure security measures

TIPS

The System Owner may consult with NUS IT Business Partner if further assistance is required



# Frequently Asked Questions

---

Here are answers to some of the most common questions we receive. If you can't find what you're looking for, please do not hesitate to contact the NUS IT Cloud Policy team at [NUSCloudPolicy@nus.edu.sg](mailto:NUSCloudPolicy@nus.edu.sg)

## Local Software & Cloud-Like Features

- ▶ I am installing software on my local computer. Do I need a cloud assessment?

No. If the software does not store or process University Data in the cloud, a cloud assessment is not required.

- ▶ We are using cloud-like features, but all data is stored and processed locally. Is a cloud assessment required?

No. If all University Data stays on your computer or on NUS-managed local systems, a cloud assessment is not required.

## Cloud Tools & Add-ons

- ▶ I want to use a free cloud tool for a student project with no University Data. Do I need a cloud assessment?

No. As long as no University Data is involved, simply inform your University Unit Head (Data Steward) and keep a record of the correspondence for audit purposes.

- ▶ If I am only evaluating or testing a cloud service without uploading University Data, do I need a cloud assessment?

No assessment is needed. Inform your University Unit Head (Data Steward) and keep a record of the correspondence for audit purposes.

- ▶ If I use a web-based tool or software, even if it's free, do I need a cloud assessment?

Yes. If University Data will be uploaded, stored, or processed by a third party, a cloud assessment is required.

- ▶ Do I need a cloud assessment for Microsoft 365 add-ons?

Partially. If the add-on does not store or process University Data in the cloud and all data is handled locally, a cloud assessment **is not required**. If any University Data is sent to or processed by external servers, a cloud assessment **is required**. To install the

add-on, submit a request to NUS IT Care to enable its installation on your account.

## Data Agreement & Purchased Data

- ▶ If a data agreement exists for external data, what should I do?

If the agreement imposes obligations on the University, treat the data as University Data and submit a cloud assessment.

- ▶ Do I need to submit a cloud assessment if I purchase data from a research survey service provider?

No, unless a data agreement or contract imposes obligations on the University regarding the data.

- ▶ How should I handle third-party survey data that is partially anonymised?

Treat it as University Data if there are contractual obligations. Submit a cloud assessment if necessary.

## Vendor Applications & Cloud Hosting

- ▶ We have a vendor developing a customised application for us, which will be hosted in the cloud. Do I need a cloud assessment?

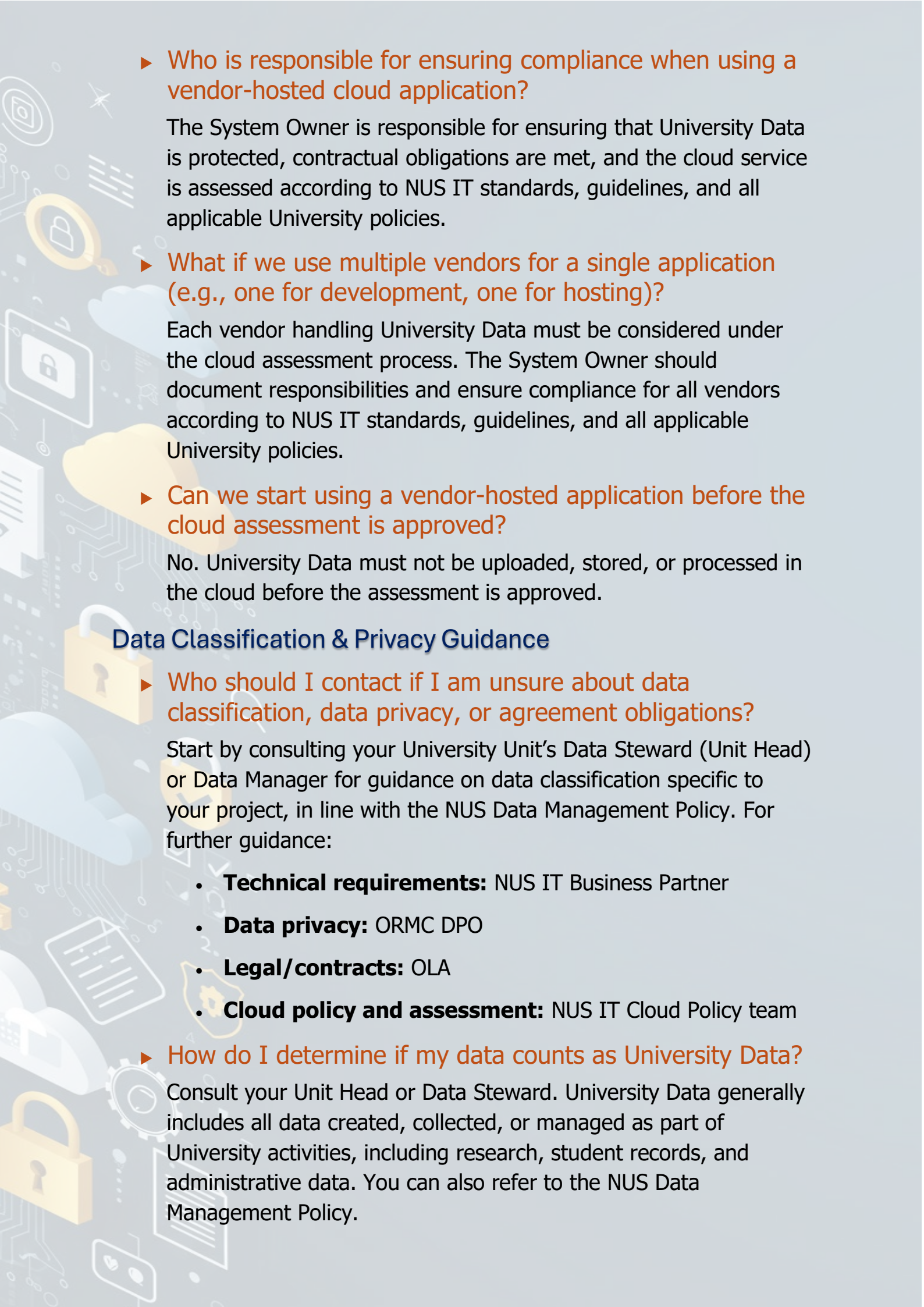
**Partially.** A cloud assessment is not required for the NUS-owned customised application itself, but it is required for the cloud hosting platform.

- ▶ What if the vendor uses subcontractors or third-party services to host or process University Data?

Yes. Any subcontractors handling University Data require compliance with cloud assessment requirements. The System Owner should ensure contractual obligations and controls are implemented according to NUS IT standards, guidelines, and all applicable University policies.

- ▶ Can we host a vendor's application on a private cloud managed by the vendor without a cloud assessment?

Partially. If University Data is involved, a cloud assessment is still required for the cloud environment. Hosting on a private cloud does not exempt the service from assessment.

- 
- ▶ **Who is responsible for ensuring compliance when using a vendor-hosted cloud application?**

The System Owner is responsible for ensuring that University Data is protected, contractual obligations are met, and the cloud service is assessed according to NUS IT standards, guidelines, and all applicable University policies.

- ▶ **What if we use multiple vendors for a single application (e.g., one for development, one for hosting)?**

Each vendor handling University Data must be considered under the cloud assessment process. The System Owner should document responsibilities and ensure compliance for all vendors according to NUS IT standards, guidelines, and all applicable University policies.

- ▶ **Can we start using a vendor-hosted application before the cloud assessment is approved?**

No. University Data must not be uploaded, stored, or processed in the cloud before the assessment is approved.

## **Data Classification & Privacy Guidance**

- ▶ **Who should I contact if I am unsure about data classification, data privacy, or agreement obligations?**

Start by consulting your University Unit's Data Steward (Unit Head) or Data Manager for guidance on data classification specific to your project, in line with the NUS Data Management Policy. For further guidance:

- **Technical requirements:** NUS IT Business Partner
- **Data privacy:** ORMC DPO
- **Legal/contracts:** OLA
- **Cloud policy and assessment:** NUS IT Cloud Policy team

- ▶ **How do I determine if my data counts as University Data?**

Consult your Unit Head or Data Steward. University Data generally includes all data created, collected, or managed as part of University activities, including research, student records, and administrative data. You can also refer to the NUS Data Management Policy.



► What should I do if my project uses non-University data?

A cloud assessment is **not required** for non-University data **unless there is a data agreement or contract that imposes obligations on the University**. In all cases, you should inform your Unit Head (Data Steward) and keep a record of the correspondence for audit purposes.

► What if University Data is anonymised or de-identified before using a cloud tool?

Yes. A cloud assessment is still required.

## Cloud Re-assessment

► When do I need to have my cloud service re-assessed?

A cloud service must be re-assessed in any of the following situations:

1. The classification of the data stored or processed by the cloud service has been upgraded to a higher sensitivity (e.g., from NUS Restricted to NUS Confidential).
2. There are significant changes to the cloud service, such as adding new modules, functionalities, or capturing additional data.
3. The cloud service provider changes their terms and conditions of service significantly.

Notwithstanding the above, if the cloud service is **critical to the success of your project**, the re-assessment shall be conducted **every 2 years**. As the System Owner, you are responsible to classify the business criticality of the cloud service and ensuring that re-assessment is duly conducted.

► If our vendor updates or modifies the cloud-hosted application, do we need a cloud re-assessment?

Yes. Significant changes to the application's functionality, data collection, or processing will trigger a re-assessment.

► What should I do if my cloud service requires re-assessment?

Submit a new cloud assessment using the NUS Cloud Assessment application, and attach all required supporting documents. **Note:** Submitting a re-assessment follows the same process as submitting a new cloud assessment.

## Cloud Security – Responsibilities & Guidance

### ► Who is responsible for cloud security when using a cloud service?

The System Owner is responsible for ensuring the cloud service is configured securely, University Data is protected, and controls are implemented according to NUS IT standards, guidelines, and all applicable University policies.

### ► What are my responsibilities as a System Owner for a cloud service?

System Owners must:

- Maintain configuration and security settings of the cloud service.
- **For IaaS/PaaS:** Apply patches and updates to mitigate vulnerabilities.
- **For SaaS:** Ensure that the CSP's patching and security updates are applied, and verify that configurations, access controls, and user permissions are correctly set.
- Conduct regular checks to ensure the cloud service complies with NUS IT standards, guidelines, and all applicable University policies.
- Report any security incidents or breaches to NUS IT immediately.

### ► Are there shared responsibilities between the University and the Cloud Service Provider (CSP)?

Yes. Cloud security is a shared responsibility. The CSP is responsible for securing the infrastructure (e.g., servers, networks), while the University (System Owner) is responsible for securing the data, accounts, access permissions, and configuration of services according to NUS IT standards, guidelines, and all applicable University policies. Please refer to [Cloud Security Responsibilities and Guidance](#) for more information.

### ► How do I maintain compliance with NUS IT cloud security guidance?

Follow the published NUS IT Cloud Security Guidelines, regularly review the cloud service configuration, and ensure your team is aware of roles and responsibilities. Consult the NUS Cloud Assessment website for more information.

## Cloud Signing-Up Information

- Is signing-up information required for the NUS cloud assessment?

No. Signing-up information provided by individual users during account creation is owned by the Cloud Service Provider (CSP) and is **not included** in the NUS cloud assessment process. Since users personally **agree to the CSP's terms of use and online privacy policies when signing up**, this information is handled directly by the CSP.

- What should I do if the department provides NUS email addresses to the CSP for account creation?

If the department provides NUS email addresses to the CSP, you should indicate this in your cloud assessment submission. This ensures **compliance and proper handling** of NUS email addresses and other personal data, if any, including obtaining **consent and permission** from each user to share their information with the CSP and confirming that they agree to the CSP's terms of use and online privacy policies.



# Useful References

---

## Relevant NUS Policies

1. [NUS Cloud Policy](#)
2. [NUS Data Management Policy](#)
3. [IT Security Policy](#)
4. [Personal Data Protection Policy and Procedures](#)

Note: This section lists only selected NUS policies relevant to the site's content. For a comprehensive list, please visit the [NUS Policy Portal](#).

## Document Templates

Please visit [NUS Cloud Assessment App](#) to download the documents under the Document Templates section.

## External Resources

1. [Guideline on Effectively Managing Security Service in the Cloud](#) by Cloud Security Alliance.

## Presentation & Videos

1. [How to Use NUS Cloud Assessment Application](#) tutorial video.