**Cloud endorsement by agency**

Agency [Please enter details]

Cloud Service [Please enter details]

Vendor [Please enter details]

From [Name, Agency Chief Information Officer; and  
Name, Agency Chief Security Officer or Chief Information Security Officer]

To [Name of Chief Executive]

Dear [Chief Executive]

I am submitting for your approval a summary of the work our agency has completed to assess the above referenced cloud service in accordance with the GCIO requirements for use of cloud services.

We are satisfied that our risk assessment is sufficient and that the residual risk has been properly accepted or mitigated. Further, we have planned ongoing assurance activities so that we and our stakeholders may maintain confidence in the cloud service into the future.

Following are some of the specific steps we completed in assessing this cloud service:

| We have: | Yes | No | Not Required | Comment |
| --- | --- | --- | --- | --- |
| Completed the GCIO’s *Cloud Computing User Assessment Tool* in line with the *Cloud Computing: Information Security and Privacy Considerations.* |  |  |  | [Please enter details] |
| Defined the information. |  |  |  | [Please enter details] |
| Classified the information. |  |  |  | [Please enter details] |
| Fully identified all entities and persons that will have access to the information / code. |  |  |  | [Please enter details] |
| Fully identified all countries / locations where the information will be stored / processed. |  |  |  | [Please enter details] |
| Reviewed security architecture documentation. |  |  |  | [Please enter details] |
| Conducted a Privacy Impact Assessment. |  |  |  | [Please enter details] |
| Completed security testing (including penetration testing if relevant). |  |  |  | [Please enter details] |
| Requested independent assurance reports (e.g. SOC 2) from the provider and reviewed them. |  |  |  | [Please enter details] |
| Requested and reviewed the design of the provider’s (and any subcontractor’s) security and privacy controls (technical and operational). |  |  |  | [Please enter details] |
| Tested / audited the design and effectiveness of provider’s (and any subcontractor’s) security and privacy controls (technical and operational). |  |  |  | [Please enter details] |
| Obtained independent verification of the provider’s claimed certifications. |  |  |  | [Please enter details] |
| Ensured contract clauses adequately address security and privacy considerations. |  |  |  | [Please enter details] |
| Discussed the solution with our external auditor to determine the impact on our annual audit. |  |  |  | [Please enter details] |
| Fully assessed ICT and business risks related to the solution. |  |  |  | [Please enter details] |
| Formally accepted the risk. |  |  |  | [Please enter details] |
| Designed and implemented mitigations for the risks not accepted. |  |  |  |  |
| Added ongoing risks to the ICT operations risk register. |  |  |  | [Please enter details] |
| Identified and scheduled assurance activities to ensure mitigations remain effective going forward. |  |  |  | [Please enter details] |
| Formally obtained accreditation for the solution. |  |  |  | [Please enter details] |

Sincerely,

Chief Information Officer

Date: day / month / year

and

Chief Security Officer (or) Chief Information Security Officer

Date: day / month / year

**After endorsement by the Chief Executive forward a copy of this document along with the *Cloud Computing User Assessment Tool* to the GCIO.**

Approved and residual risk accepted:

Chief Executive

Date: day / month / year