Cloud Computing Recordkeeping Requirements Checklist

This checklist covers recordkeeping requirements under the *State Records Act* and Standard on records management. It is recommended that NSW public offices identify any statutory requirements which apply to the records, information or data that will be created and stored in the new cloud service offering.

|  |  |
| --- | --- |
| Cloud Computing Details | *Fill in the details below to start the assessment.*  |
| Cloud Computing Service |   |
| Description of Cloud Computing Service |   |
| Business Owner |   |
| Business Area Owner |   |
| Service Provider / Vendor |   |
| Deployment model |   |
| Assessment Completed by (*Name*) |   |
|  Assessment Completed by (*Contact Details*) |   |

| NSW Cloud Computing Requirements | Requirements met?  | Action | Notes and comments |
| --- | --- | --- | --- |
|  | Yes | No | N/A | ?[[1]](#footnote-1) |  |  |
| Jurisdiction, ownership and rights over data and information |
| 1. Does the contract/agreement clearly identify your agency as the owner of the data created, transmitted, and stored with the cloud service provider?
 |[ ] [ ] [ ] [ ]  If no, negotiate with the provider to make ownership explicit in the contract / agreement. |  |
| 1. Do NSW laws apply to the contract/agreement?

Does the contract specify whether the cloud service provider also operates under another country’s jurisdiction such as the USA?*Ensure that mechanisms are in place to safeguard NSW records, data and information.* |[ ] [ ] [ ] [ ]  If no, negotiate with the provider to make NSW jurisdiction explicit in the contract / agreement. In addition, request information on how the cloud service provider manages requests for access, release or disclosure of records, information and data from those other jurisdictions.  |  |
| 1. Is any of the data or information held outside the NSW jurisdiction?

*Please note that cloud environments generally use multiple servers to store information and that these servers could be located in a computing network outside of Australia.* |[ ] [ ] [ ] [ ]  If yes, assess and mitigate risk in relation to:• potential foreign access to the data or information and its impact to the organisation’s functions and activities• potential loss of control over its safe keeping (perceived or real) and its impact on the organisation’s business processes. |  |
| 1. Does contract/agreement clearly identify:
2. rights of providers over data and information (i.e., check for clauses that mention providing rights in perpetuity)
 |[ ] [ ] [ ] [ ]  If no, request information regarding the rights of the providers over the data and information.  |  |
| 1. what data or information the cloud service providers will use
 |[ ] [ ] [ ] [ ]  If no, request information regarding the data or information the cloud service providers will use  |  |
| 1. cloud service provider’s use of NSW public office’s data
 |[ ] [ ] [ ] [ ]   |  |
| 1. extent of use, including subcontractors or third-party use
 |[ ] [ ] [ ] [ ]   |  |
| 1. intellectual property rights, specifically, where the public office and provider engage in product innovation?
 |[ ] [ ] [ ] [ ]  If no, request information regarding intellectual property rights and negotiate if necessary  |  |
| Roles a­­­nd responsibilities |
| 1. Are the roles and responsibilities of the cloud service providers and subcontractors identified and addressed or documented and transparent in relation to records and information management?
 |[x] [ ] [ ] [ ]  If yes, assess whether the information provided is sufficient for your organisation’s governance processes.If no, depending on the cloud service provider procured, public offices and the cloud service provider should identify who will define, approve, implement, monitor and review:• access controls and security measures• audit logs• systems design and metadata specifications• technical documentation• quality assurance and quality control policies, procedures and processes. |  |
| 1. Does the contract/agreement identify how your agency is/will be monitoring and managing the performance of the cloud service? Will tools be made available for your agency to verify and monitor the performance of the cloud service?
 |[ ] [ ] [ ] [ ]  If yes, retain records in official recordkeeping systems.If no, consider putting in place controls such as: • contract management system• registers such as change registers, risk registers, contract registers • recordkeeping procedures for creating and managing minutes or file notes of meetings or conversations between your agency and cloud service providers• quality assurance and control procedures • transition plans at terminations of contract/agreement. |  |
| Value, accessibility and retrieval |
| 1. Are the records, information or data stored in the cloud of high value? Is the cloud service provider supporting your organisation’s core and/or critical functions or areas which are of high risk?

*Ensure that risk mitigation strategies are in place and activated, as necessary.* |[ ] [ ] [ ] [ ]  If yes, ensure visibility by including them in your agency’s information asset register and by identifying them as specified in the NSW Cyber Security Policy.If no, identify, assess and manage potential risks to:• records, information and data• cloud service availability • information security and access• unauthorised access and release of records, information and data. |  |
| 1. Does your agency have an agreement with the cloud service provider on the format of records, data and information, including reports furnished to you?
 |[ ] [ ] [ ] [ ]  If yes, capture or save reports into your agency’s recordkeeping system or official business system. If no, specify and communicate with the cloud service provider your agency’s reporting requirements. Consider using sustainable formats to ensure accessibility of those reports. |  |
| Service management and disaster recovery |
| 1. Are tools available to your agency to verify and monitor the operation of the cloud service provider?
 |[x] [ ] [ ] [ ]  If yes, use the tools provided to monitor the performance of the cloud service. If no, check your contract and/or service level agreement whether the following are included:* monitoring tools for integrity checking, compliance checking, security monitoring and network management
* maintenance and provision of system audit logs that provide confirmation that required compliance requirements such as information protection requirements are being met
* notifications to your agency of any incidents with approved timeframes and impact assessments.
 |  |
| 1. Does the cloud service provider offer appropriate offsite back-up, disaster recovery capabilities and do they have a business continuity plan in place to safeguard your agency’s records?
 |[ ] [ ] [ ] [ ]  If yes, ensure all such measures are specified in contract/agreement - including copies of Disaster Recovery Plan and Business Continuity Plan as an appendix.If no, identify and assess your agency’s disaster recovery and business continuity requirements. Ensure that the cloud service provider puts in place measures or mechanisms to safeguard records and ensure service availability. |  |
| Sensitivity and security*For this set of requirements, we recommend engaging your organisation’s security and privacy teams to assess and verify the security measures in place for the cloud service.* |
| 1. Does the contract/agreement identify and specify that the cloud service provider has sufficient and appropriate security measures in place for handling sensitive and personal information, and security classified information?
 |[ ] [ ] [ ] [ ]  If no, ensure that the cloud service has been accredited by a relevant accreditation authority. Check Policy 11 Robust ICT systems of the Protective Security Policy Framework for more information. |  |
| 1. Have you identified what technical controls are in place over your agency’s records and related information while held by the cloud service provider and while it is in transit to or from their systems?
 |[ ] [ ] [ ] [ ]  If yes, assess whether the technical controls are sufficient. If no, consult with technical professionals within your public office or cluster who understand technical requirements for cyber security. Some of the items for consideration include:• flow filters, content filters, antivirus software• Australian Signals Directorate (ASD) approved cryptographic algorithms and protocols to protect data in transit and at rest • notifications regarding any third party seeking to have access to records |  |
| Records disposal requirements |
| 1. Is the cloud service provider able to delete information and records upon your instruction, and provide assurance or evidence that they have done so?
 |[ ] [ ] [ ] [ ]  If yes, save evidence of records deleted or disposed in official recordkeeping systems.If no, ensure that roles and responsibilities for the deletion of records, including any assurance documentation are specified in the contract/agreement. |  |
| 1. Can your agency evaluate disposal mechanisms or processes applied by the cloud service provider?
 |[ ] [ ] [ ] [ ]  If yes, ensure all such mechanisms are specified in contract/agreement.If no, identify, assess and put measures in place to ensure disposal of records are carried out as per the retention and disposal authorities. |  |
| Termination of cloud services |
| 1. Does the contract/agreement specify when, how and in what format will the cloud service provider return all required records and associated metadata? Does it specify that records and information returned or provided will be in sustainable and readable format to your organisation?
 |[ ] [ ] [ ] [ ]  If yes, ensure termination provisions are accurately and thoroughly outlined in contract/agreement.If no, specify, document, communicate and elicit agreement with the cloud service provider re: your agency’s format requirements and how data, records and information will be provided or returned. |  |

1. The “?” column indicates a situation in which additional information is needed from the vendor to sufficiently assess whether the cloud service meets the requirement. [↑](#footnote-ref-1)