Public Records Board Guidance
on the Use of Contractors for Records Management Services
Managing Records in Cloud Computing Environments

Cloud computing can be a viable alternative for storage and management of data. It can substantially reduce the infrastructure, information technology, software, and storage costs of managing electronic data and records. There can be significant benefits and risks of using cloud technology. It is imperative that the proper records management and information security controls are in place to minimize risk to units of government. This guidance will provide assistance to Wisconsin government agencies to help minimize risks and ensure the proper controls are in place before outsourcing electronic records storage and access to external cloud service providers.

Underlying Principles When Using a Third Party Contractor to Manage Records/Data

When using a third-party contractor to manage records whether in the cloud or similar service, Wisconsin government agencies have certain responsibilities based on two underlying principles:

1) Units of government are responsible for their records to the same extent whether the records are maintained by a contractor or by the government entity itself; and
2) Retention of public records is determined by their content, not the physical form in which they are maintained.

Statutory and Regulatory Compliance Considerations for the Cloud

1) Wis. Stat. 16.61 outlines the requirements for effective management and safeguarding of public records.
2) Wis. Stat. 19.35 outlines the requirements for providing access to public records.
3) Wis. Stat. 19.35(3) states that officials of Wisconsin government agencies can only charge "actual, necessary and direct costs of reproduction or transcription" to public records requestors even if the contractor charges additional fees for access.
4) Wis. Stat. 19.36(3) states that units of Wisconsin government agencies are required to provide public access to records maintained by their private contractors to the same extent as if the records were maintained by the governmental entities themselves.
5) Administrative Rule12 outlines the standards and requirements for the management of records maintained exclusively in electronic format. The rule specifically requires that Wisconsin government agencies maintain their electronic records in a secure environment for the duration of the period the electronic records must be retained.
6) Wis. Stat. 19.62-19.80 outlines requirements for managing Personally Identifiable Information (PII).

There may be additional agency-specific requirements, and/or statutes, rules or federal regulatory requirements which may impact compliance including access, security, retention, destruction and e-discovery.

Wisconsin government agencies *should ensure that all contracts provide that any disputes shall be resolved according to the laws of the State of Wisconsin.*

Staff to Engage When Developing Requirements for Cloud Service Providers

At a minimum, the following staff members should be part of the requirements development team. Additional staff members may be necessary depending on agency-specific requirements:

- Records Management/Records Officer
- Information Technology
- Information Security
- Legal
- Procurement

Ownership of Electronic Records/Data in Cloud Computing Environments

Electronic records/data and all deliverables created under the contract in a cloud service provider relationship should remain the property of the state agency or local unit of government and that should be explicitly spelled out in the contract. Electronic records/data shall not be retained, used, sold, or disseminated except as specifically outlined in the contract.

Monitoring

The Wisconsin government agencies should assess the vendor's performance and monitor the day-to-day operational requirements. To fulfill part of these responsibilities, the Wisconsin government agencies should consider requiring the cloud vendor to engage an independent auditor who can attest that the vendor's product (software, infrastructure, service) contains the proper controls and can meet the needs of the agency/local unit of government. The American Institute of Certified Public Accountants (AICPA) has established a framework to help examine controls and has established three Service Organization Control (SOC) reporting options (SOC1, SOC2 and SOC3 reports)[4].

Electronic Records Management Requirements - CHECKLIST

In accordance with Wis.Admin. Code § ADM 12.05, it is strongly recommended that the following be addressed as either requirements in the procurement document or reflected as vendor obligations in the contract

1. The contractor must maintain the electronic records so they are accurate, authentic, reliable, legible, and readable throughout the record life cycle, as that cycle is determined by state and federal law and/or the applicable approved record retention schedule.
Maintenance of Electronic Records/Data • Meet program/business area access requirements • Assure proper management of electronic records/data during provider acquisitions or divestitures • Maintain links between electronic records and its metadata throughout the record's lifecycle • Implement policies/procedures to assure compliance with requirements • Provide access to all system components for audit purposes.
Classification and Retention • Provide functionality for agency-specific classification and retention of electronic records/data in accordance with agency Records Disposition Authorizations (RDAs) and General Records Schedules • Assure electronic records/data are kept for their entire lifecycle • Implement a change management process (documented process for changing business rules, access, security, document metadata, etc.) to modify classification when RDAs or General Schedules are updated • Manage all retention types - creation (examples: creation date + 7 years, fiscal year + 6 years) and event-based (examples: date account closed + 4 years; employee termination + 6 years) • Migrate electronic records/data with long-term retention when technology/software is refreshed
Legal Hold/E-Discovery/Public (or commonly known as Open) Records Requests • Support the Legal Hold/E-Discovery/Audit/Public Records Request process according to agency-determined timelines • Flag electronic records/data responsive to a legal hold, audit, etc. • Suspend destruction/disposition of data responsive to legal hold/audit/public records request until resolved • Preserve electronic records/data and metadata for e-discovery • Resume normal destruction/disposition when legal hold/audit /public records request has been resolved
2. The contractor must guarantee it can delete or purge electronic records in accordance with approved retention schedules.
• Apply established business rules for calculating destruction • Must have agency approval prior to destroying records • Flag electronic records/data when eligible for destruction or transfer to the Archives • Schedule destruction/disposition on a regular basis • Purge flagged electronic records/data eligible for destruction • Capture destruction process in system log files • Assure that copies of electronic records/data on other mediums or in other locations are also destroyed
3. The contractor must maintain required confidentiality or restricted access conditions throughout the life cycle of the electronic records, including confidential destruction if so required.
• Provide access to electronic records/data based on disclosure requirements, including sensitive and proprietary information to avoid penalties for prohibited disclosure • Control and monitor administrative and user access to the electronic data • Capture file access, changes and deletes in system logs • Ensure that the physical machines holding the electronic data are adequately secure and that access to these machines is limited • Perform secure destruction of flagged confidential electronic records/data eligible for destruction
4. The contractor must be able to export electronic records/data that require retention to other systems without loss of meaning to produce the same result in the targeted system as in the originating environment.
• Export electronic records/data required to be transferred to the State Archives • Export electronic records/data that needs to be moved or migrated for other reasons after the normal lifecycle • Export flagged data to the State Archives or other locations without changing integrity of data or metadata

Resources

[1]"Guidance on Managing Records in Cloud Computer Environments, NARA Bulletin 2010-05 – September 08, 2010, Memo to Heads of Federal Agencies "

[2] "Guideline for Outsourcing Records Storage to the Cloud", ARMA International, 2010

[3] "Records Management Language for Contracts", National Archives, Internet, 2012

"Governance for Protecting Information in the Cloud", Blair, Barclay T., 2010 ARMA International

"Cloud Customers' Bill of Rights", Information Law Group LLP, www.infolawgroup.com, Internet, 2012

[4]"Service Organization Controls; Managing Risks by Obtaining a Service Auditor's Report", American Institute of Certified Public Accountants, Inc, (AICPA), November, 2010