OSCIO statewide policy

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

NUMBER	SUPERSEDES
107-004-150	n/a

STATEWIDE Policy

EFFECTIVE DATE	DATE OF LAST REVIEW
July 18, 2016	n/a

DIVISION

Office of the State Chief Information Officer

POLICY OWNER

Strategic Technology Office

REFERENCE/AUTHORITY

ORS 291.038

Procedure: 107-004-150 PR

SUBJECT

Cloud Computing

APPROVED SIGNATURE

Alex Pettit, State Chief Information Officer

(Signature on file with DAS Business Services)

PURPOSE

This cloud computing policy establishes standards to ensure that state agencies:

- appropriately analyze and document the benefits, costs, and risks to the state before contracting for a cloud solution;
- assess the readiness of a cloud vendor to deliver a solution that meets the state's requirements; and
- conduct planning to ensure that state information and financial assets are appropriately protected when adopting a cloud solution.

APPLICABILITY

This policy applies to all agencies within the Executive Department as defined in ORS 174.112 and includes any board, commission, department, division, or office within the Oregon Executive Department. The following agencies and boards are excluded:

- Secretary of State
- State Treasurer
- The Attorney General, but only with respect to its authority under ORS 182.124 over information systems security in the Department of Justice
- Oregon State Lottery
- State Board of Higher Education or any public university listed in ORS 352.002

FORMS, EXHIBITS & INSTRUCTIONS

These governing statutes, polices and rules must be reviewed prior to contracting for a cloud solution:

- Information Technology Investment Review/Approval Policy 107-004-130
- Information Security Policy 107-004-052
- Information Security Incident Response Policy 107-004-120
- Information Asset Classification Policy 107-004-050
- Cloud Computing Procedure 107-004-150 PR

- ORS 291.047, ORS 192.410 to 192.505, ORS 279A.157
- ORS 165.800 and ORS 646A.600 to 646A.628
- ORS 182.122 and OAR 125-800-0005 to 125-800-0020
- SB 1538 (Chapter 110, 2016 Laws)

These forms support the cloud computing purchasing process:

- Cloud Planning and Readiness Assessment Workbook, Exhibit A to this policy.
- Business case form found in the "Policies and Forms" section of the DAS web site, http://www.oregon.gov/das

DEFINITIONS

- ***"Cloud"*** has the meaning established by the International Standards Organization (ISO) standard 17788:2014: and is defined as a paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.
- ***"Cloud Services Provider"*** or ***"Vendor"*** is a contractor providing cloud services to an agency.
- ***"Cloud Services Contract"*** means the sum total of all of the documents that comprise a contract between a cloud service provider and an agency for a cloud service.
- ***"Information Asset Classification Level"*** is the classification of information by value, criticality, sensitivity, and legal implications to protect the information through its life cycle. Classification Levels are defined in DAS Policy 107-004-050 and referred to in statewide information security standards.
- ***"Public Record"*** has the meanings established in ORS 192.005 and ORS 192.410. In general it refers to information that is prepared, owned, used or retained by a state agency or political subdivision; relates to an activity, transaction or function of a state agency or political subdivision; and is necessary to satisfy the fiscal, legal, administrative or historical policies, requirements or needs of the state agency or political subdivision. It includes any writing that contains information relating to the conduct of the public's business, including but not limited to court records, mortgages, and deed records, prepared, owned, used or retained by a public body regardless of physical form or characteristics.

EXCLUSIONS AND SPECIAL EXCEPTIONS

Request exclusions to this policy by email to the Office of the State CIO (ITInvestment.Review@oregon.gov). The request should state which policy section and the exact wording to which the exclusion would apply if approved. State the limitations of the exclusion and the reasons why it is necessary and beneficial in the situation. The State CIO or designee will reply in writing with approval, denial, or limitations to the exclusion.

GENERAL INFORMATION

Strategic Considerations

The choice of a cloud solution over a custom built or agency-maintained system can have substantial, long-term impact on agency capabilities, business processes, and investments. Agencies should carefully consider the strategic implications of this sourcing decision, including how it will affect the organizational capabilities of the agency; whether the service is likely to serve agency long-term goals, and how the service and data will integrate with other state services and data to support service delivery and ongoing innovation.

Cloud solutions may present limitations or challenges for integrating data or services with other agency, state, or partner data or services. Agencies should consider how future business needs may create demands for data and service integration, and how these demands will be met. Contractual terms may be helpful in ensuring that data

and services are available for integration, for example through documented and supported Application Programming Interfaces (APIs).

In weighing alternatives, agencies should consider that cloud services are likely to align best with strategic goals when they support processes that are relatively standardized. Other approaches should be considered in cases where the agency's mission demands tight control over how the service is developed, delivered, and integrated.

Requirements

I. The selection and use of cloud computing technology or services must comply with all applicable laws, policies, procedures and standards including without limitation: privacy laws and regulations, statewide and agency specific IT security policies, internal audit controls, risk management standards, records management standards, and applicable DAS policies and procedures.

II. Before contracting for a cloud solution, the agency must complete the planning and preparation necessary to appropriately manage the associated risks. Planning should be started as soon as a cloud solution is considered, and must be carried out with diligence and rigor appropriate to the size, business impact, and risk of the proposed solution.

The Cloud Planning and Readiness Assessment Workbook published by the State CIO must be used to document the summarized results of this planning. The completed workbook, signed by both the project sponsor and the agency executive responsible for information technology, must be retained as part of the procurement file. The following risk areas must be addressed:

A. Confidentiality: Agencies must develop information security plans and cloud services contract terms to protect information to all applicable standards. At a minimum, the following apply to every cloud solution:
   - The DAS Information Security Policy (Policy 107-004-052) requires agencies to develop and implement information security plans, policies, and procedures to protect their information.
   - The Enterprise Security Office publishes statewide information security standards that define minimum requirements for information security.

B. Business continuity, data integrity, disaster recovery, and exit planning: Agencies must document their needs for business continuity, disaster recovery, and data integrity, and must develop plans and cloud services contract terms to meet those needs. Agencies must develop plans for both anticipated exit from the cloud service (such as at the end of the contract term) and unanticipated exit (in case the vendor becomes unwilling or unable to provide the service).

C. Service Management: Agencies must document their required service levels and metrics and ensure that they are appropriately represented in the cloud services contract.

D. Incident Management: Agencies must develop incident response plans and cloud services contract terms that meet their needs for incident monitoring, notification, and response. At a minimum, the following applies to every cloud solution:
   - The DAS Information Security Incident Response Policy (Policy 107-004-120) requires agencies to establish capabilities to respond to information security incidents, and requires the timely reporting of certain incidents.

E. Change Management: Cloud vendors may retain complete or near-complete control over when and how to fix defects or to add or remove software features. Agencies must evaluate this risk and consider how it can be mitigated, for example through contractual terms addressing the timing, testing, and nature of changes.

F. Public Records Management: Agencies must document the retention and destruction schedules that apply to the information stored in the cloud system, and the required ability to retrieve records as needed. Agencies must develop plans and contract terms to meet these needs and to ensure compliance with Oregon Public Records laws (ORS192.410 to 192.505) and with all other applicable federal and state statutes, rules, and policies.
   - The State Archivist is responsible for the management of public records from creation until final disposition. Agencies are required to develop policies for public records management that define the use, retention and ownership of public records and to obtain approval of those policies from the State Archivist.

G. Intellectual Property Rights: Agencies must ensure that licensing of Cloud services is consistent with the planned use of the service and that ownership of and rights to intellectual property are appropriately retained.

H. Data Ownership and Rights: Agencies must document their requirements in regards to data and metadata ownership and rights and ensure that they are appropriately represented in the cloud services contract.

I. Audits and Controls: Agencies must determine how they will assess that the vendor has appropriate controls in place and complies with legal, regulatory, and contractual commitments. The cloud services contract must include terms ensuring that appropriate audits are carried out and reports are made available, and that vendor cooperation is appropriately secured for audits by or of the agency.
   - Frameworks such as the Service Organization Controls (SOC2) or Cloud Security Alliance Controls Matrix are recommended.
   - Certifications such as the Federal Risk and Authorization Management Program (FedRAMP) may be used to facilitate agency evaluation and planning. However, certification does not substitute for agency diligence in determining the suitability of a vendor or service for a particular purpose.

III. Before contracting for a cloud solution, agencies must consider how the benefits, costs, and risks compare to the benefits, costs, and risks of alternative (non-cloud) approaches. When OSCIO approval is required (per Requirement 4, below) this consideration must be presented in the Alternatives Analysis section of the business case.

IV. If the solution meets or exceeds any of the triggering risk thresholds, the agency must obtain approval from the State CIO before contracting for the cloud solution or as required during the Stage Gate process. For complete information on risk thresholds, consult the IT Investment Policy (DAS Policy 107-004-130). Agencies must submit proposals for oversight if one or more of the following risk thresholds apply to the proposed solution:
   - it will store, process, or transmit data of Information Asset Classification Level 3 (Restricted) or higher, or information for which special protection standards apply. Examples include data protection standards under the Federal Health Insurance Portability and Accountability Act of 1996 (HIPAA), under the Federal Criminal Justice Information Services Security Policy (CJIS), or under

Publication 1075 of the Internal Revenue Service, which sets standards for protecting Federal tax information (FTI).

- it will be the system of record for information that is subject to data retention and destruction rules; or
- it will publish or be the system of record for information for which the potential cost of remediating data loss, corruption, or leakage exceeds $150,000; or
- anticipated five-year implementation and operating costs exceed $150,000.

V. Cloud services contracts must include terms and conditions required by the Attorney General in order for the contract to be approved for legal sufficiency in accordance with ORS 291.047. Cloud contracts must use available forms and templates developed by DAS and the Department of Justice in accordance with ORS 279A, including the completed contractor's insurance requirement exhibit.

This workbook forms Exhibit A to the State Cloud Computing Policy, DAS Policy 107-004-150.

For assistance in completing this Workbook, please contact your assigned Strategic Technology Officer.

The Cloud Vendor Sample Questions list maintained by the Office of the State CIO may be helpful in evaluating Clo

Privileged legal advice should not be included in this workbook.

ɔud Vendors and carrying out the Readiness Assessment.

	Cloud Planning and Readiness Assessment Workbook		
	Exhibit A to Cloud Computing Policy, DAS Policy 107-004-150		
Project name:			
Agency and Division:			
Project sponsor (name & contact info):			
	I have reviewed the answers provided here and judge that they reflect appropriate diligence and rigor.		
Sponsor Signature:			
Agency CIO/Executive in charge of IT (name & contact info):			
	I have reviewed the answers provided here and judge that they reflect appropriate diligence and rigor.		
CIO Signature:			
Date:		**Example**	**Example 2**
		Submission for final approval on a small project.	Submission as part of Stage Gate 2 approval request on a large project. For Stage Gate projects it is typical to refine planning and submit more detailed documentation over time; the answers shown here demonstrate appropriate detail for Stage Gate 2 submission, but more work needs to be done before the project is ready for Stage Gate 3 submission.
	General questions		
G1	Briefly describe the function of the proposed system.	**A cloud-based license-management package used to manage professional licenses for a board or commission**	**A cloud-based eligibility-determination system used by Oregonians, State employees, and partner organizations to apply for benefits from the State.**
G2	Does this project meet one or more risk thresholds for OSCIO oversight? Which thresholds are met? ***If "yes" approval is required from the State CIO before committing to the solution. Submit this Readiness Assessment, together with a completed Information Resource Request form and Business Case, to the Office of the State CIO.*** For complete information on thresholds, consult the IT Investment Policy. In general, oversight is required if **one or more** of the following apply to the proposed solution: a) it will store, process, or transmit data of Information Asset Classification Level 3 (Restricted) or higher, or information for which special protection standards apply. (Examples include: HIPAA, CJIS, or FTI). b) it will be the system of record for information that is subject to data retention and destruction rules; c) it will publish or be the authoritative source for information for which the potential cost of remediating data loss, corruption, or leakage exceeds $150,000; d) anticipated five-year implementation and operating costs exceed $150,000.	No. License information is public; payment information is not held in the system. The cloud system supports transactions, but official records are kept in existing internal systems & backed up with paper files as each transaction is completed.	Yes: Thresholds a, b, c, and d are all met.
	Confidentiality		
	Purpose: Limit access to those authorized, avoid data leaks or breaches.		
C1	What is the most restrictive information asset class of data that will be stored, processed, or transmitted by the cloud system? *Consult DAS Policy 107-004-050 "Information Asset Classification". If*	Level 2	Level 3
C2	List all statutory, policy, and regulatory obligations and standards related to protecting the data in question, including at minimum the Statewide Information Security Standards.	Statewide Standards	Statewide Standards, HIPAA, FTI (1075)
C3	Are there any requirements to restrict the jurisdictions in which this data may be stored or processed?	No	Yes.
C4	Have terms been included in the Cloud Services Contract to ensure appropriate treatment of the data?	Yes	Yes
	Business Continuity, Data Integrity, and Exit Strategy		
	Purpose: Manage the risks of uncontrolled changes or loss of access to the service or data.		
BC1	What are the most significant business processes supported by this system?	License renewal process.	Application process; Eligibility determination process.
BC2	What would the impact be on these processes if the service was interrupted?	License renewal applications could be accepted but renewals could not be completed.	Applications could not be accepted. Eligibility could not be determined.

BC3	What would the resultant impact be on agency operations and on Oregonians served? *Consider "worst-case" scenarios including sudden and unexpected loss of access. Include impact on the agency's ability to comply with other policies and commitments (for example, records retention and destruction policies).*	Practitioner licenses would not be renewed and might expire.. Practitioner authority to operate under Federal and State law could be impacted. A backlog of renewal applications would form.	Eligible Oregonians would be unable to obtain benefits. Demand would accrue and a glut of delayed applications would be expected upon service restoration.
BC4	Categorize the severity of these worst-case impacts. *Scale: No impact-minor impact-significant impact-severe impact.*	Significant impact.	Severe impact.
BC5	What recovery objectives are necessary in order to recover from a failure with minimal impact? *Include objectives for both recovery point and recovery time.*	Recovery point: 1 day. Recovery time: 3 days.	Recovery point: Zero loss. Recovery time: 1 day.
BC6	Estimate the likelihood of a significant unplanned loss of access, exceeding recovery objectives, during the proposed life of the system. How is this estimate supported? *Consider the vendor's performance history, SLA s, technical safeguards against interruptions, and also business and financial risks to the vendor.* *Scale: percentage likelihood of a significant event during system life.*	< 1%. The system is backed up offsite daily. It is hosted at a single location with partial redundancy (RAID storage) but no real-time failover. There is high ability to restore system within 3 days.	<0.1%. The system is built with georedundancy on platforms with 11 9's performance guarantee; vendor is a large, stable leader in the field; sophisticated change management processes are in place and included in scope of SOC 2 audit reports that are shared with us.
BC7	What is the agency's strategy to manage these risks? *Strategies may include: accepting the risk; avoiding the risk; mitigating the risk; transferring or sharing the risk. Mitigation may include, for example, plans to transfer data and service to a third party or an agency-internal fallback system, such as temporary use of paper or spreadsheet systems until service is restored.*	The agency accepts this risk. A 3-day delay in processing would have negligible impact.	The agency accepts this risk. It is not feasible to reduce this risk further regardless of sourcing strategy.
BC8	Does the agency have strategies for both planned and unplanned service exit? Briefly describe them. *Consider plans for replacing the service if necessary, plans and costs for exit, including data transfer cost and speed, data format, and vendor support through the exit process.*	No, but we plan to have monthly data dumps for import to in-house systems which will allow us to have an orderly exit to a replacement system.	No. Detailed exit planning will be conducted as we prepare for Stage Gate 3 submission.
	Service Management		
	Purpose: Optimize the processes, structures, and technologies to serve business needs. Include both those outsourced to the Vendor and those that remain with the Agency.		
SM1	What is the required system availability? *Include acceptable planned and unplanned outages with specific metrics (such as hours of downtime per month), as well as acceptable windows for planned downtime and required notice of planned downtime.*	The system should be available 99.95% of the time between 7am and midnight, Pacific time (averaged monthly). The system should be available 90% of the time between midnight and 7am. All planned and unplanned outages will be counted as "not available".	The system should be available 99.95% of the time outside of planned maintenance hours. Planned maintenance should be limited to 4 hours per week in the 2am-6am (Pacific Time) window.
SM2	What is the required system responsiveness and throughput? *Include specific metrics (such as average and peak response times by transaction type).*	95% of page loads should complete within 5 seconds.	99% of transactions should process within 10 seconds.
SM3	What are the requirements for the availability and responsiveness of support? *Include, as appropriate, the availability of self-service, the hours during which technical support is available, and target response and resolution times for support requests.*	Routine support is necessary during Oregon business hours. Outage support must be available 24/7.	Routine support is necessary during Oregon business hours. Outage support must be available 24/7.
SM4	What ability is required to scale service up or down according to agency need?	We do not anticipate a need to scale down. System should be able to scale to twice initial size within 90 days of request.	Should be able to scale down to half size or up to 4x size with 120 days notice.
SM5	Are Service Level Agreements, sufficient to meet these needs, included in the Cloud Services Contract?	Yes	We anticipate that they will be settled during contract negotiations, prior to Stage Gate 3 submission.
SM6	Are metrics objectively defined? Is authority and responsibility for monitoring and reporting on metrics appropriately recorded in the Cloud Services Contract?	Yes	Metrics are defined. Authority and responsibility for monitoring will be determined during negotiations.
SM7	Does the Cloud Services Contract include appropriate consequences for failures to meet service levels? *Consequences should be aligned with the impact of such failures on the agency, up to and including designation of significant failures as material breaches of the Cloud Services Contract.*	Yes	We anticipate that they will be during contract negotiations, prior to Stage Gate 3 submission.
	Incident Management		
	Purpose: Prepare to respond to events that impact or threaten the security and function of the system.		
IM1	Which of the following types of incidents should be addressed in agency planning for this project? -data breaches; -potential data breaches (for example, zero day vulnerabilities); -data corruption or loss; -system performance or availability issues.	Data loss, corruption, and performance/availability are significant concerns. Data in this system are generally already available to the public, so a data breach would have limited consequences.	All of the listed types.

IM2	Are the appropriate incident types adequately defined in the Cloud Services Contract?	Yes. A general description of incidents, sufficient to the proposed use, is included in the contract.	Not yet; we anticipate defining them in detail during contract negotiations before SG3 submittal.
IM3	Are notification standards adequately defined in the Cloud Services Contract? Do these standards include appropriate and objective thresholds for severity triggers and timeliness?	A general blanked standard, sufficient to the proposed use, is included in the contract.	Not yet; we anticipate defining them in detail during contract negotiations before SG3 submittal.
IM4	Are the incident management processes, and the responsibilities of each party, defined in the Cloud Services Contract?	Initial notification processes are defined. Further communications will be handled as needs arise.	Not yet; we anticipate defining them in detail during contract negotiations before SG3 submittal.
IM5	Does the Cloud Services Contract address agency needs for notification to the public or to affected users? Is the agency contractually able to control such notification?	The agency is not precluded from contacting affected users.	Not yet; we anticipate defining them in detail during contract negotiations before SG3 submittal.
IM6	Does the Cloud Services Contract address responsibilities for mitigation, remediation, and closure of incidents?	Not specifically, but there is a general "workmanlike manner" clause that provides appropriate protections.	Not yet; we anticipate defining them in detail during contract negotiations before SG3 submittal.
	Intellectual Property and Licensing		
	Purpose: Ensure that State intellectual property rights are appropriately protected and that the State complies with license terms.		
IP1	Does the licensing model support all anticipated classes of users? For example: are only State or Agency employees covered, or does the license include use by partners or the public?	Yes. The license covers all potential users of the system.	Yes, the licensing model is specifically designed to include Oregonian end-users and partner agencies as well as State employees.
IP2	Does the Cloud Services Contract ensure that agency intellectual property is retained by the agency (including materials created using the service)?	Yes. DOJ-approved IP language is included.	We anticipate including appropriate provisions in the final contract, before SG3 submittal.
IP3	Does the Cloud Services Contract appropriately restrict the vendor's use of agency intellectual property?	Yes. DOJ-approved language is included.	We anticipate including appropriate provisions in the final contract, before SG3 submittal.
IP4	If the project is federally funded, does the Cloud Services Contract secure intellectual property rights consistent with federal law?	The project is not federally funded.	We anticipate including appropriate provisions in the final contract, before SG3 submittal.
	Data ownership and rights		
	Purpose: Maintain legal protections for the information owned by or entrusted to the State.		
DO1	Identify the data and metadata that will be stored, processed, transmitted, or created by the system. be sure to include metadata, such as system-generated metadata (e.g. information about who accessed the system, when, from where, and what they did); as well as derived data about the data, such as number of users; and also aggregate and deidentified data.	Information about practitioner credentials, continuing education, and business operations, as well as derived and system-generated metadata.	Personal financial, medical, and identity information.
DO2	List the laws, rules, policies, contracts (et cetera) that govern access and rights to the data in question.	In the context of this service, all of the provided information is considered a public record.	HIPAA; IRS Pub 1075; OAR <>; ORS <>.
DO3	Does the Cloud Services Contract appropriately restrict the vendor's use of the data in question?	Yes. The vendor can only use the data and metadata for the purposes of providing the service to the State. All other uses are prohibited and all vendor rights terminate at the end of contract.	Yes. The vendor can only use the data and metadata for the purposes of providing the service to the State. All other uses are prohibited and all vendor rights terminate at the end of contract.
DO4	If rights are defined for derived, de-identified, or aggregated data, does the Cloud Services Contract clearly define appropriate standards?	n/a	n/a
	Public records management		
	Purpose: Ensure full support for maintenance of and access to public records.		
PR1	Will the proposed cloud system be the system of record for information that is subject to state retention and destruction policies? If so, describe the information in question.	No. The system supports transactions but is not the authoritative source for license information.	Yes; applications for benefits must be retained for 6 years by agency policy.
PR2	Are the retention and destruction schedules and requirements for this information clearly documented?	n/a	Yes.
PR3	Does the Cloud Services Contract include appropriate retention and destruction commitments from the vendor? Will the vendor certify destruction to specified standards? Destruction commitments must cover all copies of data including copies kept for redundancy, business continuity, and backup. Consider the necessity to support exceptions, such as the ability to freeze records for litigation holds.	n/a	We anticipate that the negotiated contract will include appropriate commitments for retention.
PR4	What are the requirements for search and retrieval of records? Requirements must be sufficient to comply with State law and policy. Include query specifications such as "full text search" or "search within a date range" or "search for messages to or from a particular email address". Include timeliness and cost of search and retrieval and the formats in which results are returned.	n/a	We anticipate that retention will be in the live system, and normal system tools will be available for search and retrieval. We have not yet addressed bulk search and retrieval options.
PR5	Does the Cloud Services Contract include appropriate commitments from vendor to cooperate with and support search and retrieval?	n/a	We anticipate that the negotiated contract will include appropriate commitments.
	Audits and controls		
	Purpose: Ensure that appropriate controls are in place to meet business objectives for service and security.		
AC1	Summarize the types of risk the vendor must address in order to meet agency risk management requirements. Risk types include at least: security, availability, processing integrity, confidentiality, privacy.	Availability and integrity risks must be managed.	Security, availability, processing integrity, confidentiality, and privacy.

AC2	Summarize the controls that the vendor will implement in order to manage these risks.	The vendor has shared recent internal audit reports describing routine backup practices including testing.	A recent SOC2 Type 2 report from the vendor is available for inspection.
AC3	How will the agency assess that appropriate controls are in place and operating effectively? Possible mechanisms: vendor audits of its own operations; agency audits of vendor operations; third party audits of vendor operations.	Annual audit reports will be required.	We anticipate contractually requiring annual audit to the same standards as the recent example.
AC4	Does the Cloud Services Contract include appropriate commitments for the nature, scope, standards, and frequency of audits, and for the timeliness and scope with which vendor or third-party results are provided to the agency?	We are using the already-shared report as an example to set the standard.	Not yet; we anticipate defining them in detail during contract negotiations before SG3 submittal.
AC5	Does the Cloud Services Contract require the vendor to cooperate with audits by or of the agency?	We do not expect that the vendor will allow audits beyond the contracted regular third-party audits.	We do not expect that the vendor will allow audits beyond the contracted regular third-party audits.
AC6	Does the Cloud Services Contract include appropriate consequences for failures to meet control commitments? *Consequences should be aligned with the impact of such failures on the agency, up to and including designation of significant failures as material breaches of the Cloud Services Contract.*	Yes	We anticipate that they will be during contract negotiations, prior to Stage Gate 3 submission.
AC7	Does the Cloud Services Contract permit the vendor to share any data or metadata with, or outsource any operations to, third parties? If so, are appropriate commitments and audits required of third parties? Must any such sharing or outsourcing be revealed?	No sharing or outsourcing permitted under our contract.	We anticipate prohibiting sharing or outsourcing by the vendor.
	Change Management		
	Purpose: Put into place processes to manage and adapt to functional changes in the Cloud system.		
CM1	Identify key functionality in the proposed system that, if changed or removed, would significantly impact Agency operations.	License management for government agencies is the core functionality of the system--much of it is key.	We anticipate defining these features in detail during contract negotiations before SG3 submittal.
CM2	Does the Cloud Services Contract include terms ensuring that this key functionality will be retained?	Since this is core system functionality, we are confident that it will be retained.	We anticipate that they will be included during contract negotiations, prior to Stage Gate 3 submission.
CM3	Does the Cloud Services Contract include terms supporting the Agency-directed development of new functionality? *Consider for example functionality that may be required for future compliance with law or policy.*	No, other than what can be achieved through configuration.	We anticipate that they will be included during contract negotiations, prior to Stage Gate 3 submission.
CM4	Does the Cloud Services Contract specify vendor responsibilities, Agency rights, and processes for managing proposed changes? *Consider: defining and prioritizing change requests; testing and release of changes; Agency choice in whether or not to accept changes.*	The vendor has a User's Group that provides input on proposed changes. There is a 90-day test period for new (non-emergency) changes.	We anticipate that they will be included during contract negotiations, prior to Stage Gate 3 submission.
CM5	Does the Agency have the internal resources and governance processes necessary to appropriately manage technical change? *Consider: impact analysis; testing; training; process optimization; vendor management.*	Yes, our technical lead is 20% dedicated to managing this vendor and system.	Yes, we will have a team dedicated to managing the vendor and the program-area IT governance; a more complete testing plan will be created as part of State Gate 4 preparation.
	Risk management and Insurance		
	Purpose: Ensure the state is adequately protected against loss in the event of data breach or loss of data or services		
RM1	Estimate agency exposure if cloud vendor experiences an illegal or unauthorized release/breach of data. How many private records will the agency be storing in the cloud? Will the vendor provide a dedicated server that holds only the agency records? If the vendor experiences a data breach, will vendor be able to tell agency if their records were affected and which ones?	We will complete the DAS Risk Management Risk Assessment tool (tabs 7 and 8 related to IT Services) to help us determine the insurance requirements of our cloud vendor contract.	We plan to store more than 500,000 records in the cloud and will contact DAS Risk Management for assistance in developing the insurance requirements for our vendor contract.
RM2	Estimate the cost to agency of uncontrolled changes or loss of access to data or services.	We will complete the DAS Risk Management Risk Assessment tool (tabs 7 and 8 related to IT Services) to help us determine the insurance requirements of our cloud vendor contract.	n/a