Software as a Service (SaaS) Strategy V1.0

March 2011
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>EXECUTIVE SUMMARY</td>
<td>1</td>
</tr>
<tr>
<td>DEFINITIONS</td>
<td>3</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>5</td>
</tr>
<tr>
<td>PURPOSE AND GUIDING PRINCIPLES</td>
<td>6</td>
</tr>
<tr>
<td>PURPOSE</td>
<td>6</td>
</tr>
<tr>
<td>GUIDING PRINCIPLES</td>
<td>6</td>
</tr>
<tr>
<td>KEY BENEFITS, RISKS AND CONSIDERATIONS</td>
<td>6</td>
</tr>
<tr>
<td>GOALS AND STRATEGIES OVERVIEW</td>
<td>10</td>
</tr>
<tr>
<td>GOALS AND STRATEGIES DETAIL</td>
<td>12</td>
</tr>
<tr>
<td>GOAL 1 – SAAS GOVERNANCE</td>
<td>12</td>
</tr>
<tr>
<td>GOAL 2 - DEVELOP ENTERPRISE SAAS SECURITY STANDARDS</td>
<td>17</td>
</tr>
<tr>
<td>GOAL 3 – STREAMLINED SAAS PROCUREMENT PROCESS AND CONTRACT REQUIREMENTS</td>
<td>20</td>
</tr>
<tr>
<td>GOAL 4 - SAAS OPERATIONAL AND TECHNICAL STANDARDS</td>
<td>22</td>
</tr>
<tr>
<td>GOAL 5 – SAAS MANAGEMENT AND REPORTING SYSTEM</td>
<td>22</td>
</tr>
<tr>
<td>APPENDICES</td>
<td>23</td>
</tr>
<tr>
<td>APPENDIX A: THE NIST DEFINITION OF CLOUD COMPUTING</td>
<td>23</td>
</tr>
<tr>
<td>APPENDIX B: ENTERPRISE INFORMATION RESOURCES MANAGEMENT STRATEGY</td>
<td>24</td>
</tr>
<tr>
<td>APPENDIX C: TEAM A’S POWERPOINT PRESENTATION</td>
<td>25</td>
</tr>
<tr>
<td>APPENDIX D: TEAM B’S POWERPOINT PRESENTATION</td>
<td>25</td>
</tr>
<tr>
<td>APPENDIX E: TEAM C’S POWERPOINT PRESENTATION</td>
<td>25</td>
</tr>
<tr>
<td>APPENDIX F: SAAS STRATEGY DOCUMENT (TEAM A)</td>
<td>25</td>
</tr>
<tr>
<td>APPENDIX G: MINIMUM SAAS VENDOR QUALIFICATIONS DOCUMENT (TEAM B)</td>
<td>26</td>
</tr>
<tr>
<td>APPENDIX H: A CANDIDATE LIST OF POTENTIAL SaaS SOLUTIONS FOR ENTERPRISE LICENSING AND INVESTMENT MATRIX (TEAM C)</td>
<td>28</td>
</tr>
<tr>
<td>APPENDIX J: LIST OF KEY RISKS AND MITIGATION ACTIONS</td>
<td>30</td>
</tr>
<tr>
<td>APPENDIX K: DATA SECURITY CONTRACT CONSIDERATIONS</td>
<td>31</td>
</tr>
<tr>
<td>APPENDIX L: SERVICE LEVEL AGREEMENTS BEST PRACTICES</td>
<td>32</td>
</tr>
<tr>
<td>APPENDIX M: IT INVESTMENT REVIEW AND APPROVAL POLICY</td>
<td>33</td>
</tr>
<tr>
<td>APPENDIX N: DAS STATE DATA CENTER EXCLUSION PROCESS/POLICY</td>
<td>34</td>
</tr>
<tr>
<td>APPENDIX O: HB 2867</td>
<td>35</td>
</tr>
<tr>
<td>APPENDIX P: TEAM A CANDIDATE LIST OF SaaS DOMAINS</td>
<td>35</td>
</tr>
<tr>
<td>APPENDIX Q: CLOUD SECURITY ALLIANCE GUIDE V 2.1</td>
<td>35</td>
</tr>
<tr>
<td>APPENDIX R: SAAS PROCUREMENT PROCESS MAP</td>
<td>37</td>
</tr>
<tr>
<td>APPENDIX S: REPORT FROM KAREN JOHNSON, DEPARTMENT OF JUSTICE</td>
<td>37</td>
</tr>
<tr>
<td>APPENDIX T: ACTION PLAN FROM TEAM B</td>
<td>37</td>
</tr>
<tr>
<td>APPENDIX U: SAAS SOLUTION SELECTION CRITERIA</td>
<td>37</td>
</tr>
</tbody>
</table>
Executive Summary

Much of state government IT exists in stove piped silos – meaning that applications and infrastructure are funded, developed, and operated in a manner independent of other IT efforts across the Enterprise or even within the same state agency. The typical approach to bringing in a new application or information system to address program needs has been to build or buy that system and install, configure, and maintain and support it internally (state staff or contractor) for many years.

The 2010 – 2015 Enterprise Information Resource Management Strategy (EIRMS) provides a roadmap for change in the management of Oregon’s information resources. The strategy calls for optimizing information investments by identifying and acting on opportunities for consolidations and shared services; reducing the complexity of the existing IT infrastructure processes and; optimizing information resource delivery across the Enterprise.

One emerging model of application hosting and deployment that holds the promise of increased efficiency, lower costs, and shorter implementation schedules is Software-as-a-Service (SaaS). The SaaS model may well provide opportunities for state government to optimize services through the innovative use of information resources. SaaS solutions may enable agencies to quickly and easily acquire essential business applications without a significant up-front capital investment in perpetual software licenses, application development costs, and additional hardware systems. Moving to a SaaS model will offer agencies the opportunity to implement solutions on an on demand - “pay by the drink”/“pay by the user” basis. On demand solutions historically have allowed organizations to avoid extended deployment cycles and added consulting and maintenance and support costs over time. The SaaS model provides a potential variety of benefits to the State including opportunities of lower cost of ownership, improved data and process performance and process consistency. However, SaaS is a model that is not without risks.

The good news is that the US General Services Administration (GSA) has taken a significant leadership role in supporting the adoption of cloud (including SaaS) computing in the federal government. In particular, GSA facilitates innovative cloud computing procurement options, ensures effective cloud security and standards are in place, and identifies potential multi-agency or government-wide uses of cloud computing solutions. GSA is also the information “hub” for cloud use case examples, decisional and implementation best practices, and sharing exposed risks and lessons learned. They have set up the Info.Apps.Gov site as an evolving knowledge repository for all government agencies to use and contribute their expertise.

The State should take advantage of the good work being done by the GSA by encouraging agencies to take a close look at solutions available on the GSA IT Schedule 70 SaaS offerings. These solutions have already been certified and accredited by the GSA and may meet minimum state security standards since they already comply with Federal Information Security Management Act (FISMA) and include FedRamp (when fully implemented) and NIST requirements. Where gaps in service offerings exist, the State should establish price agreements and contracts that make needed solutions available.

Note: The FedRamp project offers two certification levels - one suitable for “low impact” and one suitable for “moderate impact” systems’ outsourcing. Prior to SaaS solution acquisition, Oregon state agencies should examine/map the FedRamp security control certification levels against their own agency security control needs to determine whether a specific SaaS solution is a good candidate from a security point of view.
Additionally, the [Federal Cloud Computing Strategy](http://www.cio.gov/documents/Federal-Cloud-Computing-Strategy.pdf) will help to provide guidance and best practices as Oregon begins to explore both the potential and the opportunity provided by SaaS computing. The Federal Cloud Computing Strategy is designed to:

- Articulate the benefits, considerations, and trade-offs of cloud computing
- Provide a decision framework and case examples to support agencies in migrating towards cloud computing
- Highlight cloud computing implementation resources
- Identify activities and roles and responsibilities for catalyzing cloud adoption

The decision framework outlined in the Federal Cloud Computing Strategy: select, provision and manage; could well guide the State’s own decision framework.

The State should continue to monitor the Federal Strategy and take advantage of the work being done. Security, business case/decision tree templates, standards, reference architecture, taxonomy, and privacy are all areas that the Federal Government will begin developing both resources and best practices to assist agencies in cloud computing migration efforts. The State should leverage these resources as they mature and are made available to the larger government community.

The SaaS model is already beginning to emerge in the Oregon Enterprise. SaaS email services, specifically USA.net, have been implemented in some small agencies as they struggle to cut costs and work smarter with ever diminishing resources. On behalf of state government, the Department of Administrative Services (DAS) has implemented an Enterprise SaaS solution for on-line application and recruiting services (NeoGov) and provides virtual learning and audio/web conferencing environments through contracted services that offer “pay-as-you-go” solutions (AT&T and iLinc). Finally, the State of Oregon intends to enter into a Price Agreement with one or more Contractors who will provide Information Technology Capacity Brokered Data Center Services to the Oregon State Data Center (SDC). The SDC is looking to broker a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released.

This emerging SaaS and cloud-based services activity within State government calls for a concerted effort to develop and implement a SaaS strategy to assist decision makers in making smart and cost-effective decisions. Moving to a SaaS model means that the Enterprise will need to take a number of considerations into account. These include: political; technical; information security; financial and; legal/statutory considerations. Additionally, attention and direction must be given to critical areas like: Governance; Enterprise data security standards; Procurement processes, best practices and service level agreement guarantees; Operational and Technical Standards; and, Migration/Exiting strategies.

This state of Oregon SaaS Strategy has been developed to guide the acquisition, deployment, integrity, security and use of SaaS solutions within the state government enterprise. Whether a need is agency centric, commonly shared by several agencies or resides at the Enterprise level the strategy envisions a decision-making process that adheres to core principles and key criteria when making decisions related to potential SaaS implementations.
Definitions

What is Software-as-a-Service (SaaS)\(^1\)?

The National Institute of Standards and Technology (NIST) ascribe the following capability to the SaaS model: “The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure (Appendix A). The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings”\(^2\).

The SaaS model incorporates a number of unique characteristics\(^3\):

- Although the customer loses some level of control, the SaaS model shifts the burden of getting and keeping an enterprise application up and running from the customer to the vendor. It permits users to leverage the software functionality without the burden of deploying and managing the software themselves. The applications are accessed through a Web-based interface typically run from a Web browser. This delivery mechanism allows for easy scalability as new users are added.
- Generally, rather than licensing, installing and maintaining software on clients’ computers or servers, the SaaS model lets users access the vendors software via the Internet on a “pay-as-you-go” basis.
- Each customer can opt either to share access to the software with other customers (multi-tenancy), thus enabling shared total costs and creating economies of scale, or decide to be a single tenant, thus providing greater control and security.
- The SaaS model includes systematic support of the software, rather than annual maintenance and upload of fixes and patches, to all subscribers.
- The SaaS model enables every customer to benefit from the vendor’s latest technological features without the disruptions and costs associated with software updates and upgrades.
- The SaaS model eliminates the added costs and complexities of deploying additional hardware and software, or dedicating additional staff resources to support an enterprise application on an ongoing basis. (Note: The SaaS model still requires specialized staff resources who have the knowledge to manage a technical contract and work with the SaaS provider to make sure service is provided as expected).

The Hybrid Cloud Model

The Hybrid Model has arisen in response to the drawbacks of the pure SaaS model and is claimed by proponents to provide the advantages of the SaaS model, while mitigating the potential drawbacks. The Hybrid SaaS Delivery Model may be the most appropriate model for end-user organizations that have database security and or compliance issues. The hybrid model is sometimes the best solution for dealing with government regulations governing the location of databases within the enterprise jurisdiction. The traditional Hybrid SaaS model allows the customer to deploy the solution as a SaaS

---

\(^1\) The term “SaaS” has been used to describe a number of types of remote technologies and may sometimes be used synonymously with “cloud computing.”

\(^2\) The NIST Definition of Cloud Computing, Authors: Peter Mell and Tim Grance, Version 15, 10-7-09

\(^3\) “Is SaaS the Silver Lining to the Cloud”, Prashant Nema and Bronwyn Dylla Bailey, SVB, September 2, 2009
service or as on-premise solution, with the ability to switch from one to the other as needed. If deployed as a SaaS service the application may be hosted by a SaaS vendor, as a Multi-Tenanted application (i.e. available to many), and a separate database is located at each Tenant (i.e. agency) to ensure data security. Other reasons for implementing a Hybrid Model include:

- The need to store highly sensitive information
- The need for tight integration with sensitive back-end systems
- The need to transfer large files without the associated delay that can often result from the typical Internet connectivity speeds of 100kbs - 1000kbs, as compared to internal Ethernet speeds of up to 1,000,000kbs
- Concerns about the long term financial viability of any given SaaS vendor
- The need to modify (customize) the core software itself
- Preference for paying a lump sum rather than monthly hosting charges

**Horizontal Application**

A **horizontal application** is a software package designed to be used by many different kinds of organizations and individual users. In terms of the SaaS strategy, horizontal applications refer to applications that will be used by all /multiple agencies.

**Vertical Application**

A **vertical application** is a software package designed to be used by a single market. In terms of the SaaS strategy, vertical application refer to applications that will be used by single agencies for particular needs specific to the agency program area.

**SaaS Implementation Levels of Need**

**Agency Centric:** If the business need is unique to a single agency or if other agencies having the same business need are neither prepared nor incentivized to migrate to a SaaS solution (i.e. vertical application for a single agency, recent implementation of an on-premise system, legacy system in use, etc) then the SaaS solution should be considered Agency Centric. In this case the solution decision may be quick and the path from procurement to implementation should be as easy and smooth as possible.

**Common (across several agencies):** Multiple agencies may identify a common business need that could be addressed by a candidate (horizontal application) SaaS solution. In this case business owners from across the common agencies will need to come together to determine if an appropriate SaaS solution is available. The decision process is longer but once a solution is determined, the procurement to implementation process should be as streamlined as possible.

**Enterprise Level:** If the business need serves all (or nearly all) agencies (i.e. Fleet Management; Facilities Management; Procurement, Human Resources, Finance System, etc) any proposed solution should first be categorized an Enterprise level solution. Again, business owners and stakeholders from across the enterprise will need to come together to determine the appropriate path for any potential SaaS solution to Enterprise business needs.

An Enterprise level solution by nature will have the longest decision process due to many factors including complexity, number of stakeholders, criticality and the like. However, once a solution is determined the procurement to implementation process, while lengthy, should be as streamlined as possible.
**Background**

The 2010-2015 Enterprise Information Resource Management Strategy (EIRMS) development effort was led by DAS on behalf of the agencies of state government (Appendix B). The conclusions, goals, and strategies in the document were collaboratively developed. The update occurred at a time of unprecedented challenges to citizens and the state government services upon which they rely. Those challenges continue today. The EIRMS provides a multi-agency framework to address the full range of challenges while also producing the added value of predictably optimizing overall cost, effectiveness and efficiency of information resources.

The Vision of the EIRMS states: “Oregon government services are optimized through the innovative use of information resources.” The EIRMS document describes a vision for the strategic management of information resources over a six-year planning horizon. It anticipates a combination of actions to allow agencies to work together to identify and act to optimize:

- Agencies’ business processes and support systems;
- Better target agencies’ resources on achieving missions and business objectives; and
- The cost, efficiency and effectiveness of information resources overall.

The strategy provides a road map for change in the management of Oregon’s information resources.

SaaS is an emerging model of application development and deployment. The SaaS model may well provide opportunities for Oregon government to optimize service delivery through the innovative use of information resources including opportunities of lower cost of ownership, improved data and process performance and process consistency.

In order to ensure the state is able to take advantage of the potential value of the SaaS model and SaaS solutions, a SaaS strategic plan is necessary. Developing a SaaS strategy that guides the exploration of and potential migration to a SaaS model, is in alignment with the following goals and strategies of the EIRMS:

**EIRMS Goal 2: OPTIMIZE information investments.**

- **Strategy 2.1:** Identify and act on opportunities for consolidation and shared services
- **Strategy 2.2:** Reduce the complexity of the existing IT infrastructure and processes
- **Strategy 2.3:** Optimize DAS and agency information resource delivery

**EIRMS Goal 3: INNOVATE service delivery and improve access to government services and information.**

- **Strategy 3.1:** Improve citizen interaction with government services and information
- **Strategy 3.2:** Establish capabilities to evaluate, prototype, and pilot potential innovative solutions and risk strategies

As an initial step toward developing a comprehensive Enterprise SaaS Strategy, a multi-agency SaaS Strategy and Brokering IT Contracts Workshop was held on October 14 and 15, 2009. The workshop was sponsored by Dugan Petty, State Chief Information Officer, and facilitated by Ben Berry, ODOT Chief Information Officer, and ODOT Staff. The workshop participants divided into three teams with specific tasks as follows:
Team A – SaaS Strategy: Team A was tasked with creating a stakeholder-based consensus driven state SaaS strategy. (Team A’s report - Appendix C)

Team B - Saas Procurement Process: Team B was tasked with using waste identification and process improvement methodology to reduce the non-value added time in SaaS procurement. (Team B’s report - Appendix D)

Team C - Brokering IT Contracts: Team C was tasked with producing a stakeholder driven consensus decision on SaaS applications for enterprise licenses. (Team C’s report - Appendix E)

At the conclusion of the workshop each team presented their findings and recommendations to the larger group. The following deliverables were a result of those presentations:

- Draft SaaS Strategy Document (Appendix F)
- Minimum SaaS Vendor Qualifications Document (Appendix G)
- A candidate list of potential SaaS solutions for enterprise licensing (Appendix H)

Purpose and Guiding Principles

Purpose
This SaaS strategy represents the methodology and process guidelines for the ongoing acquisition of SaaS solutions at the enterprise and agency levels.

Guiding Principles
The principles guiding the EIRMS implementation over time should also serve to guide the SaaS strategy and any future implementation of the SaaS model (Appendix I). Those principles are:

- **Interoperable Enterprise** – The agencies of the State of Oregon should function as an interoperable enterprise.
- **Timely Results** – Agencies derive value from effective and efficient use of affinity groups, enterprise collaboration, and multi-agency sharing to deliver timely results transparently.
- **Stakeholder Value** – Enterprise efforts are driven from the perspective of stakeholder value.
- **Build On Success** – Successful approaches are replicated or built on to improve results.
- **Value of Standardization** – Agencies recognize the value of standardization to reduce risk, increase value, provide consistency, improve efficiency and reduce or avoid cost.
- **Security** – Agencies respect the public trust by protecting the security and integrity of the public’s information.
- **Innovation and Risk** – Strategically balance efforts to manage risk and the innovative use of information resources to produce greater value, efficiency, and effectiveness.

Key Benefits, Risks and Considerations

SaaS solutions have both short and long-term benefits. SaaS solutions enable agencies to quickly and easily acquire essential business applications without a significant up-front capital investment in perpetual software licenses and additional hardware systems. They also avoid extended deployment cycles and added consulting and support costs. SaaS solutions have also been specifically designed to be more flexible and accessible for a highly dispersed and variable workforce than legacy applications. However, SaaS solutions are not without risks (See Appendix J for more details).
Key Benefits and Risks of SaaS Solutions:

- **Short-term benefits:**
  - Accelerated software deployment with generally less risk. Quicker time to deployment (value)
  - Lower up-front costs. Higher productivity/ROI, at a lower Total Cost of Ownership (TCO)
  - No additional hardware and lower internal staffing requirements for system implementation, maintenance and support
  - May provide greater reliability, security and privacy but tradeoffs must be considered
  - Greater agility to scale software to meet changing business requirements
  - Immediate, easy wins for proof of concept projects across the Enterprise
  - Successful proof of concept projects will validate and inform the longer term SaaS strategy
  - Opportunity to “lean” the state procurement process to better advantage the SaaS benefit of a short implementation cycle
  - Ability to re-allocate IT resources from legacy systems to more strategic projects

- **Long-term benefits:**
  - Resource efficiency gains
  - Quality of Service improvements, (citizen service improvements)
  - Reduced risk as compared to conventional project/system development methods
  - Lower total cost of ownership
  - Business process alignment across the Enterprise

- **Risk Factors**
  - Difficult to achieve agency agreement on common functions, solutions and procurement process
  - Threat of employee job loss--cultural change-impact to workforce
  - Transition from legacy system to multi-tenant, shared system or other hybrid SaaS model
  - Unable to realize savings that might result from SaaS deployment due to need for cost recovery of State Data Center (SDC) investment
  - Potential lack of alignment/interoperability with existing technology/data sharing environment
  - Potential complexity/risks associated with data management, security and privacy. Potential loss of data or data breach -- Public Records, Privacy
  - Time consuming legacy procurement process that may not fit acquisition of SaaS offerings
  - Inability to determine TCO of the SaaS Solution
  - The potential impact associated with the need to change vendors (disentanglement)
  - Vendor support and reliability over time
  - Executive Approval--executives burned at the stake for taking risks
  - Funding and budget process – moving from a capital investment to an operational expense
  - Potential legislative opposition to hosting SaaS solutions and state data in out of state locations
  - General loss of control of provisioning and operational processes -- from personnel practices through data handling practices to policies to operational procedures.

Considerations

Moving to a SaaS Model means taking a number of considerations into account, each of which ultimately boils down to a tension between control and cost. Some of these considerations include the following:

- **Political considerations.** Sometimes, the decision can be short-circuited by resistance from within an organization, if key program and technology leaders insist that certain functionality remain internal, or under the control of IT; other considerations therefore become unimportant.
• **Technical considerations.** SaaS applications typically provide some flexibility for customer configuration, but this approach has its limitations. If an important application requires specialized technical knowledge to operate and support, or requires customization that a SaaS vendor cannot offer, it might not be possible to pursue a SaaS solution for the application. Another factor to consider is the type and amount of data that will be transmitted to and from the application on a regular basis. Internet bandwidth pales in comparison to the gigabit Ethernet links commonly found in enterprise LANs, and data transmissions that take a few seconds or minutes to transfer between servers in your server room might take minutes or hours to transmit to and from a SaaS application located across the country. Because of this, it might make sense to consider a solution that takes network latency into consideration. An appliance-based solution, for example, might cache or batch locally.

• **Financial considerations.** Consider the TCO of a SaaS application, compared to that of an equivalent on-premise application. Although the initial cost of acquiring software capabilities through SaaS is normally lower than that of on-premise applications, the long-term cost structure is less certain. Factors that can affect the TCO of a SaaS application include the number of licensed users; the amount of custom configuration needed to integrate the SaaS application with the on-premise information systems/infrastructure; and whether or not existing data centers already provide economy of scale, thereby reducing the potential cost savings of SaaS. Consider, too, “soft costs” to outsourcing decisions, such as the potential loss of “knowledge capital” and loss of gains due to innovation and internal improvement, or of additional costs due to time- and distance-imposed communication difficulties (i.e. offsite or out-of-country support personnel).

• **Legal considerations.** Some government agencies are subject to higher regulatory/statutory requirements, which may impose various reporting and recordkeeping requirements that your potential SaaS solution candidates cannot satisfy. Consider the regulatory environments in all the different jurisdictions in which state government operates and how these affect agency application needs. The different jurisdictions in which the SaaS provider operates should also be considered, particularly if a provider has international operations. International legal and regulatory differences can present significant complexity.

Sometimes, technical and financial considerations also can have legal ramifications, such as whether candidate SaaS providers will be able to meet the internal standards for data security and privacy in order to avoid legal exposure. Consider any legal obligations toward customers or other parties, and whether SaaS will allow the agency to continue to meet them.

**Other considerations/implications**
Performing due diligence is a routine part of any successful IT infrastructure deployment project. Some areas to address in any due-diligence checklist include:

• **Data-security standards.** Moving critical business data "outside the walls" introduces a risk of data loss or inadvertent exposure of sensitive information. Oregon state agency customers will need to review and assess statewide and agency security standards and the agency data-security needs, and ensure that the provider has measures in place to meet the standards set. *(See Appendix K for a list of Data Security Contract Considerations)*

• **Service Level Agreement (SLA) guarantees.** The management contract between the enterprise/agency and the SaaS provider takes the form of service-level agreements (SLAs) that guarantee the level of performance, availability, and security that the SaaS vendor will provide, and govern the actions the provider will take—or the compensation it will provide—in the event that it fails to meet these guarantees. Ensure that these SLAs are in place, that the guarantees they make are sufficient to meet agency needs, and that they provide a sufficient level of mitigation in even the worst-case scenario. *(See Appendix L for a list of SLA Best
Practices). Also plan for the loss in flexibility that contractual guarantees may bring – negotiating a contract change order may impede the ability to respond to changing circumstances.

- **Migration/Exiting strategies.** At some point, an agency might want to migrate away from a SaaS application to another solution, so it's important that the agency is able to take their existing data out of the application and move it to another one. Ask the prospective SaaS provider about any data-migration strategies and procedures it uses, including any provisions for data and code escrow.

- **In-house integration requirements.** Ensure that migrating to SaaS will meet any functional and data-integration requirements the agency/organization has in place.

- **Reporting services.** Because SaaS involves giving up direct control of some of the agency data, accurate and useful reporting is especially important. Determine what reporting services the provider offers, and whether they are compatible with the agency business-intelligence requirements.

- **Auditing requirements.** Because SaaS requires giving up control of many aspects of how data is handled, the ability to audit the SaaS vendor’s handling practices to ensure compliance with contractual and legal requirements is important.

- **Adherence to the IT Investment Review and Approval Policy** (Appendix M)
- **DAS State Data Center (SDC) Exclusion Process/Policy** (Appendix N)
- **Satisfying HB2867 requirements for professional services contracts that exceed $250,000.** (Appendix O)
Goals and Strategies Overview

The following goals express the results the state of Oregon hopes to achieve through this SaaS strategy:

**GOAL 1**  
SaaS GOVERNANCE

Strategy 1.1: Establish or utilize an existing Executive-Level Governance Body to set priorities for selection, procurement, and implementation of SaaS solutions (at the Agency, Common, and Enterprise level).

Strategy 1.2: Establish Key Criteria and Core Principals for making decisions about SaaS and to determine level of need:
- Agency Centric, Common (across several agencies), Enterprise Level

Strategy 1.3: Periodically, bring together stakeholders, subject matter experts and business owners to review business needs and available SaaS solutions and make recommendations to the Executive level governance body regarding solutions that may be worth pursuing at the multi-agency or state level.

Strategy 1.4: Once a solution and need level have been identified, bring appropriate business owners and stakeholders together to identify which, if any, SaaS Hybrid Models are appropriate for the successful sourcing and implementation of the identified candidate domain.

Strategy 1.5: Identify the appropriate SaaS architecture for the candidate Hybrid Models and develop short and long-term implementation plans for each.

Strategy 1.6: Develop a SaaS Migration Strategy and measures for success of SaaS implementations

Strategy 1.7: Leverage the SDC price agreement for Brokered Data Center Services for Infrastructure as a Service (IaaS)

**GOAL 2:**  
ENTERPRISE SaaS SECURITY STANDARDS

Strategy 2.1: Work with ESO to determine minimum security standards for SaaS implementation at each need level (i.e. Agency Centric, Common, and Enterprise)

- Utilize National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA) standards to inform state standards over time. NIST plans to issue technical security guidance, such as that focused on continuous monitoring for cloud computing solutions, consistent with the six step Risk Management Framework.

- Assess solutions offered by GSA IT Schedule 70 to ensure they meet minimum state security standards outlined within the DAS Information Security Plan and Standards documents. Note: GSA IT Schedule 70 SaaS Solutions are assumed to comply with Federal Information Security Management Act (FISMA) and include FedRamp and NIST requirements.

---

5 https://cloudsecurityalliance.org/
6 http://www.nist.gov/itl/csd/guide_030210.cfm
GOAL 3:
STREAMLINED SaaS PROCUREMENT PROCESS AND CONTRACT REQUIREMENTS

Strategy 3.1: DAS to deploy a SaaS Provisioning Website with links to SaaS tools and services available through GSA IT Schedule 70 and the State Procurement Office (SPO)

- Note: A candidate list of potential SaaS solutions for enterprise licensing (Appendix H) was developed as part of a multi-agency SaaS Strategy and Brokering IT Contracts Workshop held on October 14 and 15, 2009. This short, mid and long-term candidate list of SaaS solutions should serve as an initial guide for posting on this SaaS Provisioning website and for future procurement efforts designed to establish statewide price agreements for SaaS solutions.

Strategy 3.2: Develop SaaS contract requirements in alignment with GSA and SPO

Strategy 3.3: Develop a list of Best Practices for SaaS contracts and Service Level Agreements

Strategy 3.4: Develop a funding model that allows agencies to flexibly pursue SaaS Solutions through a shift from a traditional capital outlay expense to operational expenses for services over time.

Strategy 3.5: Create a leaner SaaS procurement process that allows for a reduced solicitation cycle time to execute enterprise SaaS agreements.

Strategy 3.6: Identify the top essential and desirable criteria for selecting vendors.

GOAL 4:
SaaS OPERATIONAL AND TECHNICAL STANDARDS

Strategy 4.1: Align with current Operational and Technical Standards of SDC

Strategy 4.2: List of Best Practices for SaaS Operational Standards for implementation at each level (i.e. Agency Centric, Common need, Enterprise Need).

Strategy 4.3: List of Best Practices for SaaS Technical Standards for implementation at each level (i.e. Agency Centric, Common need, Enterprise Need).

Strategy 4.4: Align with Agency and DAS adopted architectures and standards to ensure systems and data interoperability

GOAL 5:
SaaS MANAGEMENT AND REPORTING SYSTEM

Strategy 5.1: Develop a SaaS Management and Reporting system at DAS, EISPD that ensures:
- Continuous awareness of state government’s access to and use of SaaS Solutions
- Ability to assess alignment with Enterprise IRM Strategy and agency strategic goals and objectives
- Ability to assess opportunities for leveraging resources and cutting costs
- Ability to assess performance of SaaS solutions
- Ability to refine selection criteria, and security, operational and technical standards based on Oregon’s experience with SaaS solutions over time.
Goals and Strategies Detail

GOAL 1 – SaaS Governance

Strategy 1.1: Establish or utilize an existing Executive-Level Governance Body to set priorities for selection, procurement, and implementation of SaaS solutions (at the Agency, Common, and Enterprise level).

Discussion – Identifying an appropriate governance body is critical to the short and long-term success of the SaaS strategy. In this case, governance implies a system in which all stakeholders, including executive management, customers, and staff have clear accountability for their respective responsibilities in the decision making processes affecting the overall SaaS Strategy.

Once identified, the Governance body should work with DAS to:

- Amend or edit IT governance policies to create high-level guidelines that address the specific aspects of purchasing, deployment and managing of SaaS applications as solutions to defined business needs.
- Draft a SaaS-specific governance policy to maximize cost effectiveness & business value and minimize risk and exposure when selecting, purchasing and deploying SaaS applications, and to make sure agencies align these decisions with agency and enterprise business goals and needs.
- Encourage agency issuance of policies that apply/govern agency centric SaaS solutions, rather than depending solely on compliance with State IT Policies.

Strategy 1.2: Establish Key Criteria and Core Principals for making decisions about SaaS and determine level of need.

Discussion – How are decisions about SaaS going to be made? Who will make them? What if an agency needs to replace an application that is at the end of its lifecycle? What if several agencies need a new application to address new or changing common business needs? What are the criteria for making specific decisions? These and other questions will need to be addressed very early to ensure that SaaS decisions are both thoughtful and smart. A group of business owners and stakeholders from across the Enterprise will need to come together to develop, and as necessary codify, the key criteria and core principals essential for making smart SaaS decisions.

Once a business need has been identified and vetted through the key criteria, business owners and stakeholders will need to determine which SaaS applications are potential candidate solutions and determine the level of need. There are three levels of need that should be considered for any SaaS implementation. They are:

- Agency Centric: If the business need is unique to a single agency or if other agencies having the same business need are neither prepared nor incentivized to migrate to a SaaS solution (i.e. vertical application for a single agency, recent implementation of an on-premise system, legacy system in use, etc) then the SaaS solution should be considered Agency Centric. In this case the solution decision may be quick and the path from procurement to implementation should be as easy and smooth as possible.
- Common (across several agencies): Multiple agencies may identify a common business need that could be addressed by a candidate (horizontal application) SaaS solution. In this case business owners from across the common agencies will need to come together to determine if an appropriate SaaS solution is available. The decision process is longer but once a solution is determined, the procurement to implementation process should be as streamlined as possible.

- Enterprise Level: If the business need serves all (or nearly all) agencies (i.e. Fleet Management; Facilities Management; Procurement, Human Resources, Finance System, etc) any proposed solution should first be categorized an Enterprise level solution. Again, business owners and stakeholders from across the enterprise will need to come together to determine the appropriate path for any potential SaaS solution to Enterprise business needs. An Enterprise level solution by nature will have the longest decision process due to many factors including complexity, number of stakeholders, criticality and the like. However, once a solution is determined the procurement to implementation process, while lengthy, should be as streamlined as possible.

**NOTE:**
For multiple agencies using a shared software instance, stakeholders should come together to identify the horizontal and vertical application domains.

An **horizontal application** is a software package designed to be used by many different kinds of organizations and individual users. In terms of the SaaS strategy, horizontal applications refer to applications that will be used by all/multiple agencies.

A **vertical application** is a software package designed to be used by a single market. In terms of the SaaS strategy, vertical application refer to applications that will be used by single agencies for particular needs specific to the agency program area.

SEE DIAGRAM ON NEXT PAGE
SaaS Strategy Decision Process v1.0

Core Principles
- Aggregate the demand for the benefit of all
- Protect legacy systems and investments when appropriate
- Make smart, effective decisions
- Data interoperability and data sharing are essential
- Streamline the overall procurement to implementation process, especially for agency-centric needs

Governance

Key Criteria

Determine Need

Agency Centric Need

Agency Business Owner Determines SaaS Solution

EISPD/E-Gov stand up site with links to SaaS tools available through GSA/SPO

DAS IT Investment Review and Approval (Information Resource Request—IRR)

SaaS Offering

Common Need (Across several agencies)

Business Owner and Stakeholders come together to determine common need

No

Yes

Determine SaaS Solution

Determine SaaS Solution

DAS IT Investment Review

SaaS Offering

Enterprise (Finance System; Facilities Management, Fleet Management etc)

Business Owner and Stakeholders come together to determine need

Determine SaaS Solution

DAS IT Investment Review

SaaS Offering

SaaS Offering

SaaS Offering

SaaS Offering

Management System & Reporting

Security Requirements (Agencies/ESO)

Streamlined Procurement Process & Contract Requirements (NISST/GSA/SPO)

Technical Standards & Operational Standards (SDC)
Strategy 1.3: Periodically, bring together stakeholders, subject matter experts and business owners to review business needs and available SaaS solutions and make recommendations to the Executive level governance body regarding solutions that may be worth pursuing at the multi-agency or state level.

Discussion – A candidate list of potential SaaS domains (e.g. HR, Compliance, Collaboration, Document Management, Finance, etc.) was developed by Team A (See Appendix P). This initial list of SaaS solution domain areas should be reviewed and updated over time based on Executive level governance body decisions.

Strategy 1.4: Once the solution and need level have been identified, bring appropriate business owners and stakeholders together to identify which, if any, SaaS Hybrid Models are appropriate for the successful implementation of the identified candidate domain.(see also Cloud Security Framework in Strategy 3.1)

Discussion – SaaS systems can be configured and delivered using several different delivery models to cover a multitude of deployment approaches. SaaS Software can be hosted off-premises (in the cloud), on-premises (at the end user organization), or as a 'hybrid' configuration with the database/data hosted/stored on-premises while the application is hosted in the cloud. Each candidate domain should be reviewed to determine the level of security necessary to protect the asset (data, application, function or process). Hybrid SaaS solutions take advantage of many of the SaaS benefits while allowing the business owners to maintain control of the critical assets and information as business requirements dictate. To effectively evaluate a potential hybrid deployment the agency and/or Enterprise should have a rough architecture in mind of where components, functions, and data of the candidate domain should/will reside.

Strategy 1.5: Identify the appropriate SaaS architecture for the candidate Hybrid Models and develop short and long-term implementation plans for each.

Discussion – A properly architected SaaS system should offer a variety of installation/configuration options in order to satisfy differing customer security/governance/control requirements. It is also possible to design an application as a 'dual-mode' (On-premises + SaaS) system. Enterprise business owners and stakeholders will need to come together to determine the appropriate SaaS configuration for any given application that is a candidate for current and/or future SaaS implementations at the enterprise level. Similarly, agency business owners and stakeholders will need to collectively determine the appropriate SaaS configuration for Common/Agency Centric applications to be deployed for use at the agency level. Once determined, short and long-term implementation plans will need to be developed to ensure success.

Strategy 1.6: Develop a SaaS Migration Strategy

Discussion – Key to the development of any kind of SaaS roadmap is an inventory/evaluation of the existing information systems environment, identifying candidate information systems that could be offered via, Software as a Service, and conducting an honest assessment of the opportunities and threats this approach may introduce into the agency or enterprise business and technical operating environment.

SaaS adoption demands significant technical and operational capabilities. Assessing the current and required capabilities of the organization and the SaaS provider, will help fill the gaps and prepare for a successful implementation. A small pilot or proof-of-concept project may prove invaluable at the early phase of adoption. A limited implementation can often validate the approach taken and expose any key challenges and complexities.
The following are six key steps to a successful SaaS migration strategy:

1. Learning - Both the technical and non-technical staff involved in policymaking positions need to learn about cloud computing and the potential it holds.
2. Organizational Assessment - Conduct an examination of the organization’s real IT utilization and how cloud-based storage, applications, and processing power might replace or supplement present IT capacity.
3. Cloud Pilot - Use one project—perhaps on the edge of the organization—to test how cloud works for your agency and with your existing technology and people.
4. Cloud-Readiness Assessment
5. Cloud Rollout Strategy - Integrate cloud offerings as part of the agency’s overall IT strategy and work to gain buy-in to the change effort throughout the organization.
6. Continuous Cloud Improvement - Cloud resources become part of the everyday workings of the agency, and as they do, these will necessitate making decisions as to when and how to best make use of cloud based storage and application solutions.

**Strategy 1.7:** Leverage the DAS State Data Center (SDC) price agreement for Brokered Data Center Services for Infrastructure as a Service (IaaS)

**Discussion** – The State of Oregon intends to enter into a Price Agreement with one or more Contractors who will provide Information Technology (“IT”) Capacity Brokered Data Center Services to the Oregon State Data Center (SDC). The SDC desires to periodically outsource certain IT services during the term of this Price Agreement.

The SDC is looking to broker a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released.

---

7 Moving to the Cloud: An Introduction to Cloud Computing in Government, David C. Wyld, IBM Center for the Business of Government
GOAL 2 - DEVELOP ENTERPRISE SaaS SECURITY STANDARDS

Strategy 2.1: Work with ESO to determine minimum security standards for SaaS implementation at each need level (i.e. Agency Centric, Common, and Enterprise)

Discussion – According to the National Institute of Standards and Technology (NIST) there are three critical requirements for cloud computing: Interoperability, Portability and Security. While high quality mature standards could facilitate a smoother transition to cloud computing, the development of such standards is a consensus oriented process that can often take years to complete. Even longer for international standards.

NIST has advised that until cloud computing standards mature what is needed is a process to test the three critical cloud system requirements of portability, interoperability and security.

Interoperability: to ensure clouds work together
- Formats for data import and export (e.g., XML schemas)
- Interfaces, Semantics, Programming Models

Portability - so workloads can move around
- If necessary can the data be quickly and securely migrated back to the Enterprise (i.e. the SaaS vendor goes out of business)
- If necessary can the customer switch SaaS providers
- If necessary can the customer move components of the SaaS offering back and forth from the SaaS hosting location to internal data center locations.

Security: to ensure that agency security risk is managed appropriately in the SaaS provider’s computing environment

According to Gartner, there are (at least) 7 primary security risks a customer should consider:

1. Privileged user access. Sensitive data processed outside the enterprise brings with it an inherent level of risk, because outsourced services bypass the "physical, logical and personnel controls" IT shops exert over in-house programs. Get as much information as you can about the people who manage your data. Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access,

2. Regulatory compliance. Customers are ultimately responsible for the security and integrity of their own data, even when it is held by a service provider. Traditional service providers are subjected to external audits and security certifications. Cloud computing providers who refuse to undergo this scrutiny are signaling that customers can only use them for the most trivial functions.

3. Data location. When you use the cloud, you probably won't know exactly where your data is hosted. In fact, you might not even know what country it will be stored in. Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers.

4. Data segregation. Data in the cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure-all. Find out what is done to segregate data at rest. The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists. Encryption accidents can make data totally unusable, and even normal encryption can complicate availability.

---

5. **Recovery.** Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster. Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure. Ask your provider if it has the ability to do a complete restoration, and how long it will take.

6. **Investigative support.** Investigating inappropriate or illegal activity may be impossible in cloud computing. Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers. If you cannot get a contractual commitment to support specific forms of investigation, along with evidence that the vendor has already successfully supported such activities, then you’re only safe assumption is that investigation and discovery requests will be impossible.

7. **Long-term viability.** Ideally, your cloud computing provider will never go broke or get acquired and swallowed up by a larger company. But you must be sure your data will remain available even after such an event. Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application.

More comprehensive guidance is available from the Burton Group - “Implementing Security Controls In Outsourced Environments” (Nov. 11, 2010 – Eric Maiwald).

Agencies should consult with their own internal Information Security staff as well as the Enterprise Security Office for advice and counsel on this topic prior to procuring a solution and deploying it for use within their agency environment. Part of any decision to acquire and deploy a SaaS solution should include performing a risk assessment to determine how the risk picture will change and what new risks are introduced by the decision to utilize a SaaS solution. Any planning to utilize a SaaS solution should include risk mitigation methods to compensate for the additional risk, including agreements with the vendor for compensating controls. Any SaaS Solution procured/deployed for use by state government agencies must meet Oregon’s Enterprise Security Standards or meet GSA Federal Information Security Management Act (FISMA)/ NIST/FedRamp standards for SaaS Solution information security.

**Standards Unique to Cloud Computing:**
- Federated security (e.g. identity) across Clouds
- Metadata and data exchanges among Clouds
- Standards for describing resource/performance capabilities and requirements
- Standardized outputs for monitoring, auditing, billing, reports and notification for Cloud applications and services
- Common representations (abstract, APIs, protocols) for interfacing to cloud resources
- Cloud-independent representation for policies and governance
- Portable tools for developing, deploying, and managing Cloud applications and services
- Orchestration and middleware tools for creating composite applications across Clouds

The need for security standards development in each of these areas for all potential SaaS models (e.g. public, private, and hybrid) should be discussed with the Office of the State CIO and with the members of the state’s CIO Council and other appropriate IT related governing bodies. As needed, workgroups should be formed to develop and recommend standards for state CIO adoption.

In addition, National Institute of Standards and Technology (NIST) and Cloud Security Alliance (CSA) standards should be used to inform state standards development over time. (See Appendix Q) for information related to the Cloud Security Alliance and NIST.
US General Services Administration (GSA) IT Schedule 70 SaaS offerings

The US General Services Administration (GSA) has taken a significant leadership role in supporting the adoption of cloud computing in the federal government. They have concentrated their efforts on facilitating easy access to cloud based solutions from commercial providers that meet federal requirements, enhancing agencies’ capacity to analyze viable cloud computing options that meet their business and technology modernization needs, and addressing obstacles to safe and secure cloud computing.

In particular, GSA facilitates innovative cloud computing procurement options, ensures effective cloud security and standards are in place, and identifies potential multi-agency or government-wide uses of cloud computing solutions. GSA is also the information “hub” for cloud use case examples, decisional and implementation best practices, and sharing exposed risks and lessons learned. They have set up the Info.Apps.Gov site as an evolving knowledge repository for all government agencies to use and contribute their expertise. Federal Information Security Management Act (FISMA) requirements are binding on all federal agencies, so all information systems, including cloud computing that agencies deploy must comply with it. All offerings under IT Schedule 70 related to identity and access management, (in particular SIN 132-60 A-E) are required to meet the “medium” FISMA standards for Identity and Access management.

The GSA is in the final stages of shoring up the requirements for a government-wide program to certify and accredit cloud computing products and services. The agency has issued Version 2 of the Federal Risk and Authorization Management Program (FedRAMP) requirements. Version 2 of the FedRAMP requirements will include security controls detailed in the National Institute of Standards and Technology's Special Publication 800-53R as well as enhancements. FedRAMP is an interagency effort whose aim is to reduce duplicate efforts and security compliance expenditures, as well as encourage rapid acquisition time frames, security oversight, and consistent integration with federal government-wide security efforts.

Note: SIN 132-60: Access Certificates for Electronic Services (ACES) Program. This program provides identity management and authentication services and ACES digital certificates for use primarily by external end users to access Federal Government electronic services and transactions in accordance with the X.509 Certificate Policy for the Federal ACES Program.

Prior to acquisition, state agencies should evaluate and assess SaaS solutions offered by GSA IT Schedule 70 to ensure they meet minimum state security standards. Note: GSA IT Schedule 70 SaaS Solutions are assumed to already comply with Federal Information Security Management Act (FISMA) and include FedRamp and NIST requirements.
GOAL 3 – STREAMLINED SaaS PROCUREMENT PROCESS AND CONTRACT REQUIREMENTS

Strategy 3.1: DAS to deploy a SaaS Provisioning Website with links to SaaS tools and services available through GSA IT Schedule 70 and the State Procurement Office (SPO)

Discussion – Following the model established by the GSA, the state of Oregon should establish a SaaS/Cloud Services website to increase and maintain state and local government agency awareness of available SaaS/Cloud solutions. This website should progressively evolve from a static listing of available/soon to be available offerings to an actual provisioning storefront through which state and local government agencies can order services. The site should include links to SaaS tools and services available through GSA IT Schedule 70 as well as price agreements negotiated through the SPO. Alternatively, the state of Oregon should work with GSA to enable Oregon state and local government agencies access to Apps.Gov.

- Note: A candidate list of potential SaaS solutions for enterprise licensing (Appendix H) was developed as part of a multi-agency SaaS Strategy and Brokering IT Contracts Workshop held on October 14 and 15, 2009. This short, mid and long-term candidate list of SaaS solutions should serve as an initial guide for posting on this SaaS Provisioning website and for future procurement efforts designed to establish statewide price agreements for SaaS solutions.

Strategy 3.2: Develop SaaS contract requirements in alignment with GSA and SPO

Discussion – The Federal Government plans to facilitate an “approve once and use often” approach to streamline the approval process for cloud service providers. The GSA’s Infrastructure as a Service (IaaS) contract award is an example of this “approve once and use often” approach. It offers 12 approved cloud vendors to provide agencies with cloud storage, virtual machines, and web hosting services. Approaches such as this will eliminate unnecessary cost and delivery delays associated with duplication of effort.

As the number of government cloud providers increases, GSA will provide comparison tools to transparently compare cloud providers side-by-side. These tools will allow all government agencies to quickly and effectively select the best offering for their unique needs. Examples include Apps.gov, which provides a centralized storefront where agencies can easily browse and compare cloud SaaS offerings from previous Multiple Award Schedule (MAS) 70 contract holders. Tools such as these will reduce the burden on government agencies to conduct their own RFP processes and will concentrate investments in the highest-performing cloud providers.

Furthermore, GSA is establishing contract vehicles for government-wide commodity services (e.g., email). These contract vehicles will reduce the burden on agencies for the most common IT services. GSA is also creating working groups to support commodity service migration. These working groups will develop technical requirements for shared services to reduce the analytical burden on individual government agencies. For example, the SaaS E-mail working group established in June 2010 is synthesizing requirements for government-wide e-mail services. Working groups are also creating business case templates for agencies that are considering transitioning to cloud technologies.

Federal Government contracts will provide riders for state and local governments. These riders will allow all of these governments to realize the same procurement advantages of the Federal Government. Increasing membership in cloud services will further drive innovation and cost efficiency by increasing market size and creating larger efficiencies-of-scale.
The GSA plays a significant leadership role in supporting the adoption of cloud computing in the federal government. They have concentrated their efforts on facilitating easy access to cloud based solutions from commercial providers that meet federal requirements, enhancing agencies’ capacity to analyze viable cloud computing options that meet their business and technology modernization needs, and addressing obstacles to safe and secure cloud computing. In particular, GSA facilitates innovative cloud computing procurement options, ensures effective cloud security and standards are in place, and identifies potential multi-agency or government-wide uses of cloud computing solutions. GSA is also the information “hub” for cloud use case examples, decisional and implementation best practices, and sharing exposed risks and lessons learned. They have set up the Info.Apps.Gov site as an evolving knowledge repository for all government agencies to use and contribute their expertise.

The State Procurement Office (SPO) should take the lead on establishing the processes, procedures, and contract templates for state of Oregon SaaS and Cloud Computing services and work with agencies to mature them over time. These processes, procedures and contract templates should align to the greatest extent possible with those already developed by GSA.

**Strategy 3.3:** Develop a list of Best Practices for SaaS contracts and Service Level Agreements (SLA’s)

**Discussion** – Gartner recommends that SAAS contracts include clauses for disaster recovery, data security and privacy, exit and merger and acquisition protections, uptime (the amount of time the application is actually functional), performance service-level agreements, penalties and incentives, and pricing (including issues related to renewal).

The management contract between the enterprise/agency and the SaaS provider takes the form of service-level agreements (SLAs) that guarantee the level of performance, availability, and security that the SaaS vendor will provide, and govern the actions the provider will take—or the compensation it will provide—in the event that it fails to meet these guarantees. Ensuring that these SLAs are in place, that the guarantees they make are sufficient to meet enterprise/agency needs, and that they provide a sufficient level of mitigation in even the worst-case scenario are critical to the success of any SaaS implementation. A regularly reviewed and updated list of “Best Practices” for SaaS Contracts and SLA’s should be maintained by SPO and shared with all agencies considering and/or participating in SaaS procurements and implementations. (See Appendix L)

**Strategy 3.4:** Develop a funding model that allows agencies to flexibly pursue SaaS Solutions through a shift from a traditional capital outlay expense to operational expenses for services over time.

**Discussion** – Typically, state agencies budget for the procurement and deployment of information systems (hardware and software) within the capital outlay portion of their agency budgets. Once the legislatively adopted budget for the agency has been set, it can be difficult for some agencies to move monies allocated within these budget categories to operational (services and supplies) categories. A funding model that removes this kind of administrative barrier is needed whereby agencies can efficiently and timely pursue software as a service (SaaS) offerings when the business case to do so has been made.

**Strategy 3.5:** Create a leaner SaaS procurement process that allows for a reduced solicitation cycle time to execute enterprise SaaS agreements.

**Discussion** – IT contracting processes will need to evolve and focus on unique aspects of SaaS and Cloud Computing as compared to traditional information systems acquisition, deployment, ownership, maintenance and support within the agency/enterprise hosting environment. A leaner SaaS procurement process is needed to enable agencies and the enterprise to effectively and efficiently pursue SaaS and Cloud Computing opportunities. Updates to contract terms and conditions are required to meet business needs and business models of SaaS solution providers in the marketplace.
During the initial SaaS Workshop, held in October 2009, Team B developed a streamlined procurement process model that was expected to reduce the SaaS solicitation cycle time by an estimated 37% (from 121 days to 76 days).

- See the full SaaS Procurement Process Map in Appendix R
- See DOJ email from Karen Johnson, Sr Assistant Attorney General (Appendix S)
- See the full Action Plan (using SaaS email as a model) in Appendix T

**Strategy 3.6:** Identify the top essential and desirable criteria for selecting vendors.

**Discussion** – A SaaS Solution’s Selection Criteria should be developed that is applicable to both horizontal and vertical applications where possible. See Appendix U for more detail:

**GOAL 4 - SaaS OPERATIONAL AND TECHNICAL STANDARDS**

**Strategy 4.1:** Align with current Operational and Technical Standards of SDC

**Discussion** – Any SaaS Solution should align as closely as possible with the current Operational and Technical standards that exist within the DAS State Data Center (SDC). The SDC Consolidation Architecture Governing Principles document serves as a good foundation for agencies to review prior to pursuit of a SaaS Solution. [http://www.oregon.gov/DAS/SDC/docs/architecture/Governing_Principles.pdf](http://www.oregon.gov/DAS/SDC/docs/architecture/Governing_Principles.pdf)

As agencies and the state as a whole gain more experience with the selection, acquisition, deployment and use of SaaS Solutions, Best practices for SaaS Operational and technical standards should be developed.

**Strategy 4.2:** Develop a list of Best Practices for SaaS Operational Standards for implementation at each level (i.e. Agency Centric, Common need, Enterprise Need).

**Strategy 4.3:** Develop a list of Best Practices for SaaS Technical Standards for implementation at each level (i.e. Agency Centric, Common need, Enterprise Need).

**Strategy 4.4** Align with Agency and DAS adopted architectures and standards to ensure systems and data interoperability

**GOAL 5 – SaaS MANAGEMENT AND REPORTING SYSTEM**

**Strategy 5.1:** Develop a SaaS Management and Reporting system at DAS, EISPD that ensures:

- Awareness of state government’s access to and use of SaaS Solutions
- Agency compliance with DAS IT Investment Review and Approval Process
- Ability to assess alignment with Enterprise IRM Strategy and agency strategic goals and objectives
- Ability to assess opportunities for leveraging resources and cutting costs
- Ability to assess performance of SaaS solutions
- Ability to refine selection criteria, and security, operational and technical standards based on Oregon’s experience with SaaS solutions over time.
APPENDICES

Appendix A: The NIST Definition of Cloud Computing

Authors: Peter Mell and Tim Grance
Version 15, 10-7-09

National Institute of Standards and Technology, Information Technology Laboratory

Note 1: Cloud computing is still an evolving paradigm. Its definitions, use cases, underlying technologies, issues, risks, and benefits will be refined in a spirited debate by the public and private sectors. These definitions, attributes, and characteristics will evolve and change over time.

Note 2: The cloud computing industry represents a large ecosystem of many models, vendors, and market niches. This definition attempts to encompass all of the various cloud approaches.

Definition of Cloud Computing:

Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service’s provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, laptops, and PDAs).

Resource pooling. The provider’s computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, network bandwidth, and virtual machines.

Rapid elasticity. Capabilities can be rapidly and elastically provisioned, in some cases automatically, to quickly scale out and rapidly released to quickly scale in. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.

Measured Service. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported providing transparency for both the provider and consumer of the utilized service.
Service Models:

*Cloud Software as a Service (SaaS).* The capability provided to the consumer is to use the provider’s applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

*Cloud Platform as a Service (PaaS).* The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

*Cloud Infrastructure as a Service (IaaS).* The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

*Private cloud.* The cloud infrastructure is operated solely for an organization. It may be managed by the organization or a third party and may exist on premise or off premise.

*Community cloud.* The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be managed by the organizations or a third party and may exist on premise or off premise.

*Public cloud.* The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

*Hybrid cloud.* The cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load-balancing between clouds).

*Note:* Cloud software takes full advantage of the cloud paradigm by being service oriented with a focus on statelessness, low coupling, modularity, and semantic interoperability.

**Appendix B: Enterprise Information Resources Management Strategy**

[http://www.oregon.gov/DAS/EISPD/docs/Reports/0_EIRMS_20100129_1400_FINAL.pdf](http://www.oregon.gov/DAS/EISPD/docs/Reports/0_EIRMS_20100129_1400_FINAL.pdf)
Appendix F: SaaS Strategy Document (Team A)

What is a SaaS Strategy?
The Software as a Service (SaaS) strategy represents the methodology and process guidelines for the ongoing acquisition of SaaS solutions.

This document is designed to help agencies understand the importance of having a SaaS strategy at an enterprise level for the State of Oregon, as well as the benefits these solutions can provide for short and long term. On the other hand, the document deals with the multiple risk factors the stakeholders can face and details strategies for addressing them.

Why is it important?
A SaaS strategy is important for the State of Oregon because of multiple reasons:
- Federal, State and Local software adoption is experiencing a significant environmental impact change. In September of 2009 the Obama administration launched the General Service Administration’s Cloud Store front of SaaS applications at Apps.gov.
- State and federal mandates that no longer business as usual, and it is anticipated by 2014 the majority of software produced in the US will be delivered from the “cloud” as on-demand, SaaS or some hybrid.
- There are a variety of benefits to the State including opportunities of lower cost of ownership, improved data and process performance and process consistency. On demand solutions historically have provided reduced maintenance costs, faster implementation and adoption times. This strategy provides the opportunity to foster consistency of software applications across agencies, improve quality and efficiency and reduce risk.
- This movement of providing for the adoption of SaaS solutions will allow the State to leverage emerging inter-state synergies and best practices.
What are the short and long term benefits?

- **Short-term benefits:**
  - Immediate, easy wins for proof of concept
  - Validate the longer term SaaS strategy
  - Opportunity to “lean” the state procurement process
  - Ability to re-allocate IT resources for more strategic projects

- **Long-term benefits:**
  - Resource efficiency gains
  - Quality of Service improvements, (citizen service improvements)
  - Reduced risk for conventional project development
  - Lower total cost of ownership
  - Cross functional transparency
  - Business process alignment

Who are the stakeholders affected?

When implemented the SaaS strategy will affect various internal as well as external stakeholders. The identified categories of affected stakeholders are:

1. Agency business owners
2. Citizens
3. CIO’s
4. IT staff
5. Enterprise business owners
6. Legislature (must adopt budget perspective)
7. Local government/Federal government

Long Term Strategies

- Effective/Efficient Procurement Process
- Effective ongoing menu of SaaS services (available online)
- Stakeholder engaged governance
- At some point having all stakeholders provide input for a hybrid model
- A funding model that allocates funding for a SaaS model. (Requirement for re-allocation of funding methodology)
- Appropriate development of standards for SaaS solutions

Appendix G: Minimum SaaS Vendor Qualifications Document (Team B)


1. **Financial Competency**
   a. Profitability
   b. Cash-flow
   c. Debt level
   d. ROI/cost benefit justification
   e. Tiered pricing
   f. Cost effectiveness for customers (short /long term)
   g. Tiered services (modules)
   h. Procurement method availability (Will vendor agree to state terms and conditions for SAAS or resell through resell contract?)
2. Technical Competency
   a. Data portability and interoperability
   b. Availability
   c. Statewide scalability
   d. Ease of use
   e. Ease of implementation
   f. Domain expertise for government usage/references
   g. Security competency/Security compliance
   h. Dedicated storage flexibility
   i. Disaster recovery plan/business continuity
   j. Exit strategy in the event the State or agency chooses to discontinue use of the service.
   k. Vendor able to provide the architectural design to maximize efficiency of service
   l. Technology integrates with existing systems if needed
   m. Technology fits into the statewide architecture plan
   n. User configurable
   o. Meets or exceeds functionality requirements
   p. In line with Enterprise or agency authority
   q. Cost of standard implementation and configuration
   r. Proof of concept availability
   s. Is customization necessary and at what cost?

3. Training and support
   a. 24x7 support
   b. Service level agreements (SLA) guaranteeing uptime and availability of service (i.e., % of SaaS fees refunded to state for SLA breach
   c. Upfront and on-going training
   d. Pilot support
   e. Executive sponsorship
   f. Hotline, email, etc. support flexibility
   g. Onsite professional services availability if required

Others to consider: Public records law
## Appendix H: A candidate list of potential SaaS solutions for enterprise licensing and Investment Matrix (Team C)

<table>
<thead>
<tr>
<th>1. EMPLOYEE PERFORMANCE MANAGEMENT</th>
<th>e.g. Success Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. HR BPO (INCLUDE TIME AND ATTENDANCE: OFLA, FEMLA)</td>
<td>Include Time and Attendance: OFLA, FEMLA</td>
</tr>
<tr>
<td>3. UNIFIED COMMUNICATION</td>
<td>e.g. Microsoft's Business Productivity Online Standard Suite, Google Apps and Unisys Unified Communications</td>
</tr>
<tr>
<td>4. EMAIL ARCHIVING</td>
<td>e.g. USA.net; Proofpoint; Sonian Archive SA2</td>
</tr>
<tr>
<td>5. FINANCIAL ACCOUNTING</td>
<td>e.g. GovCount; Financial Force.com</td>
</tr>
<tr>
<td>6. ASSET ACCOUNTING</td>
<td></td>
</tr>
<tr>
<td>7. ERP</td>
<td>e.g. NetSuite; SAP ERP</td>
</tr>
<tr>
<td>8. E-PROCUREMENT</td>
<td>e.g. Enporion e-Procurement</td>
</tr>
<tr>
<td>9. PROCURE TO PAY</td>
<td>e.g. Ariba Procure-to-Pay</td>
</tr>
<tr>
<td>10. INFRASTRUCTURE SERVICE (NON MISSION CRITICAL)</td>
<td>e.g. Windows Azure; Cloudstack; Amazon Web Services</td>
</tr>
<tr>
<td>11. ENTERPRISE CONTENT MANAGEMENT</td>
<td>e.g. SpringCM; enChoice</td>
</tr>
<tr>
<td>12. FLEET MANAGEMENT</td>
<td>e.g. Telogis' Fleet Management</td>
</tr>
<tr>
<td>13. RELATIONSHIP MANAGEMENT</td>
<td>e.g. Salesforce.com; Sage CRM</td>
</tr>
<tr>
<td>14. TRAVEL EXPENSE</td>
<td>e.g. Concur Travel and Expense</td>
</tr>
<tr>
<td>15. WEB CONFERENCING</td>
<td>e.g. AT&amp;T Connect, iLinc, Adobe Connect, IBM Lotus Live; ReadyConference; Visioncast MS Live Meeting</td>
</tr>
<tr>
<td>16. CASE MANAGEMENT (SINGLE AGENCY VIEW)</td>
<td></td>
</tr>
<tr>
<td>17. DESKTOP OFFICE PRODUCTIVITY TOOLS</td>
<td>(e.g. MS BPOS, Google Apps; Open Office.org)</td>
</tr>
</tbody>
</table>
Appendix I: More About Guiding Principles

Principles
Several principles have been developed to guide strategy implementation over time; answering questions that have not yet been asked.

Interoperable Enterprise – The agencies of the State of Oregon should function as an interoperable enterprise.
- The enterprise acts as a thoughtful, well-intentioned whole to optimize cost, resources and efficiency.
- Agencies strive to understand and optimize what is common with other agencies and with other jurisdictions.
- Planning, budgeting, funding processes are conducive to solving enterprise problems.

Timely Results – Agencies derive value from effective and efficient enterprise collaboration that delivers timely results.
- Lead on behalf of the enterprise or affinity group.
- Collaboration, sharing, transparency and trust are paramount.
- The value of enterprise activities increases the earlier they are deployed in the planning process. Optimum value is derived by inventorying agencies' business needs, then deploying enterprise solutions based on those common business needs.
- Repetitive development effort is neither productive nor cost-effective.
- Use appropriate technology to extend service delivery.
**Stakeholder Value** – Enterprise efforts are driven from the perspective of stakeholder value.
- Business models and funding models are aligned around citizen and agency value.
- Enterprise efforts are outcome based. Target outcomes are established early.
- Progress toward outcomes is measured and tracked.
- The governance of enterprise information resource management involves key stakeholders on an ongoing basis. Governance should focus on supporting those who guide and authorize state government operations. Governance should engage the right people at the right time for appropriate reasons including: state executive and legislative decision-makers; agency heads; administrative leaders; technology leaders; subject matter experts; and stakeholders. Stakeholders’ business requirements drive enterprise action

**Build On Success**
- Successful agency project managers lead enterprise efforts.
- Successful funding models are replicated.
- Successful collaboration models are expanded.
- Successful individuals act as mentors for others.
- Successful strategies and solutions are repeated wherever it makes sense.
- Successful platforms are leveraged and expanded.

**Value of Standardization** – Agencies recognize the value of standardization of back office functions.
- To reduce risk, increase value, provide consistency, improve efficiency and reduce or avoid cost.

**Appendix J: List of Key Risks and Mitigation Actions**

<table>
<thead>
<tr>
<th>Risk Factors</th>
<th>Mitigation Actions</th>
<th>Designated party to take action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agency Agreement on Common Functions-Administrative Functions not valued</td>
<td>Master Change Facilitation to come to agreement. Workshops with stakeholders to come to common understanding.</td>
<td>Individual agency and Enterprise level</td>
</tr>
<tr>
<td>Threat of Employee Job Loss--cultural change-Impact to Workforce</td>
<td>Cost Benefit Analysis, Part of Communications strategy, outreach to staff and the unions</td>
<td>Enterprise level</td>
</tr>
<tr>
<td>Transition</td>
<td>Develop a Transition Plan, incorporate terms and conditions in documents in how we would make a transition,</td>
<td>Individual agency and Enterprise level</td>
</tr>
<tr>
<td>SaaS deployments not hosted at SDC may negatively impact economies of scale and rates for shared SDC computing environment.</td>
<td>Work with SDC finance committee, Cost Benefit Analysis, TCO considering sunk costs and planning cycles, prior investment made</td>
<td>Individual agency</td>
</tr>
<tr>
<td>Existing Technology Inconsistency</td>
<td>Developing Standards for SaaS applications</td>
<td>Enterprise level</td>
</tr>
<tr>
<td>How to manage the data -- privacy</td>
<td>Applying Information Security Architecture Standards for SaaS applications</td>
<td>Individual agency and Enterprise level</td>
</tr>
<tr>
<td>Risk Factors</td>
<td>Mitigation Actions</td>
<td>Designated party to take action</td>
</tr>
<tr>
<td>-------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------</td>
</tr>
<tr>
<td>Ineffective Procurement Process</td>
<td>Crafting a Procurement Process that is calculated to achieve the outcomes that is necessary to achieve this strategy. Ensure agencies know how to state their requirements in a SaaS offering through an online menu of SaaS applications readily accessible to state agencies to establish an account.</td>
<td>DAS- SPO (State Procurement Office)</td>
</tr>
<tr>
<td>Lack of ability to determine TCO (ST)</td>
<td>Establish a few key common performance indicators &amp; metrics for the TCO model. Establish baseline for candidate SaaS opportunities</td>
<td>DAS- SPO (State Procurement Office) Enterprise level</td>
</tr>
<tr>
<td>Lack of Data Interoperability</td>
<td>Establish a requirement with the SaaS vendor, evaluation prior to the purchase</td>
<td>DAS- SPO (State Procurement Office)</td>
</tr>
<tr>
<td>Changing vendors</td>
<td>In the contract process mitigate these risks for an exit strategy</td>
<td>DAS- SPO (State Procurement Office)</td>
</tr>
<tr>
<td>The complexities and lead time for getting agreement with agencies to allow clear pathways for procurement process</td>
<td>Published SaaS procurement process</td>
<td>DAS- SPO (State Procurement Office)</td>
</tr>
<tr>
<td>Vendor support and reliability</td>
<td>Establish a requirement with the SaaS vendor, evaluation prior to the purchase (financial statements, backbone of the company)</td>
<td>DAS- SPO (State Procurement Office)</td>
</tr>
<tr>
<td>Executive Approval--executives burned at the stake for taking risks</td>
<td>Formal agency buy-in and endorsement as you go. (When you roll out programs start with small pilot, staged approach)</td>
<td>Enterprise level</td>
</tr>
<tr>
<td>Funding and Budget Process</td>
<td>Partner with BAM and LFO to develop a funding strategy and alternatives for SaaS that would be discussed with legislative committee</td>
<td>Enterprise level</td>
</tr>
<tr>
<td>Legislative Opposition</td>
<td>Education, Socializing, Early successes, staged approach with pilot</td>
<td>Enterprise level</td>
</tr>
<tr>
<td>Potential Loss of Data or Data breach -- Public Records, Privacy. Is the information on the system secure? What are the security issues?</td>
<td>Established in the contract, must meet DAS security standards and policies. Assessment and evaluation to comply with state and federal laws and communicated with vendor in the contract SLA’s. Understanding the risk going in at the RFP stage versus the contract stage. Understanding the inherit risk of the data model.</td>
<td>DAS- SPO (State Procurement Office)</td>
</tr>
</tbody>
</table>

**Appendix K: Data Security Contract Considerations**

To protect enterprise data, the State may wish to consider the following for any software or managed service contract:

- Uptime percentage guarantees (some companies are putting "clawbacks" into their contracts, specifying discounts for uptime shortfalls)
- Advance system maintenance notifications specifying whom to notify and how far in advance
- Outage notifications that include full problem description and a resolution/escalation plan.
- Documented disaster recovery and business continuity plans
- Data backup procedures, including schedules for incremental and full backups
- Restore procedures for lost data
- Network access protection policies and procedures
- Technical support services and procedures
- Code fix and upgrade procedures including practices for mitigating and notifying customers of security vulnerabilities identified in provided service
- Procedures for returning or destroying data (some exceptions may be made for secured application backups)
- Regulatory considerations for certain data types (for example, health information)
- Timely notification to customer of potential data breaches in provided service, including those in other provided services that may affect the customer
- Restricting ownership of company data to the company
- Restricting vendor from de-encrypting or viewing company data except when absolutely necessary
- Company data on vendor’s mobile devices must be protected in transit and at rest
- Code escrow provisions
- Workforce and physical security procedures to prevent unauthorized access or data theft
- Workforce practices to produce and maintain secure software offerings
- Device and media controls and policies to protect data
- Data transmission security policies and procedures
- System and security monitoring tool usage
- Requirements to allow 3rd-party audit of security controls

**Appendix L: Service Level Agreements Best Practices**

The management contract between the enterprise/agency and the SaaS provider takes the form of service-level agreements (SLAs) that guarantee the level of performance, availability, and security that the SaaS vendor will provide, and govern the actions the provider will take—or the compensation it will provide—in the event that it fails to meet these guarantees. Ensuring that these SLAs are in place, that the guarantees they make are sufficient to meet your needs, and that they provide a sufficient level of mitigation in even the worst-case scenario are critical to the success of any SaaS implementation. The following are some recommended best practices for ensuring the SLA provides the kind of protection and guarantees needed to ensure success.

**Control oriented Service Level Agreement Terms**
- Establish a system availability SLA, based on average monthly availability, with bonuses for overachieving and increasingly steep penalties for downtime beyond the agreed level.
- Establish a system response time SLA, based on average monthly response time, with penalties for slow system performance.
- Establish a fail over window for disaster recovery SLA in the case of a catastrophic failure of the vendor's infrastructure.

**Operational Risk oriented Service Level Agreement Terms**
- Ensure that you can get your data back if you ever decide to leave and that it is unambiguous that you own your data.
- Ensure that the vendor will assist you in migrating away, for an appropriate professional services fee.
- Ensure that you can retain your data on the vendor's system for an appropriate fee if you ever need to stop using the service but don't want to lose access to your data.
- Review the vendor's privacy policy and make sure that you understand what happens according to the SLA if there is ever a privacy breach.
- Ensure that the vendor undertakes annual SAS70 Type II audits, and that the vendor further undergoes annual third party security and penetration testing.
Business Risk oriented Service Level Agreement Terms

- Establish an error resolution time SLA, with different windows for different severity levels (system down vs. workaround) and again with penalties for not being responsive.
- Establish criteria for the quality and timeliness of professional services engagements with bonuses for implementations that go better than planned and penalties for those that do not.
- Look for guarantees around proactive communications - look for monthly product feature updates and quarterly roadmap updates and understand how your requests for new features and product changes will be prioritized.
- Ask for money-back guarantees - cloud vendors may be willing to offer you a money-back guarantee, particularly if you are willing to commit to a pre-agreed upon scope of work and criteria for success. If you are comparing multiple vendors this can be a great way to reduce your risk or at least to understand how confident the vendors are that they will meet your needs.

Penalties / Rewards and Transparency oriented Service Level Agreement Terms

- In each of the above sections, ensure that the vendor documents the methodology for measuring performance and calculating penalties and rewards.
- Understand whether you will be issued an automatic credit if a failure occurs that impacts you, or must you ask your vendor for a credit to receive one.
- Understand whether you can you get out of your contract if the vendor continuously and materially fails to meet their SLA.
- Ensure the vendor guarantees transparency and proactive notification of system availability, production issues, scheduled downtime and pending updates.
- Review the vendor's public real-time status website that shows their operational performance. If they don't have one, think about looking for another vendor.
- Review the vendor's published service level agreement and understand how it applies to you (and how it compares to this list). If the SLA isn't published on the company’s website, that may be a red flag.

Appendix M: IT Investment Review and Approval Policy

Information Resource Request (IRR) Review Criteria

The Department of Administrative Services (DAS), through the State Chief Information Officer, uses IT investment review and approvals to answer the following critical questions:

a) Does the proposed IT investment aligned with the Governor’s Priorities and initiatives, the Enterprise Information Resources Management (EIRM) Strategy, the Oregon Strategic Plan for Geographic Information Management, the Enterprise Security Plan and standards, the State Data Center Strategic Plan, the E-government Transition Plan, and other related statewide plans, initiatives, goals and objectives?

b) Does the proposed IT investment align with/support agency business plans?

c) Is the IT project being pursued because of a federal or state mandate?

d) Is there a sound business case for the proposed IT investment?

i. Has the case clearly defined what the case is about, the purpose for the proposed solution, what business problems the proposed solution attempts to solve, and the scope of the proposal?

ii. Has the cash flow, the flow expenditures, and the intake of financial benefits been presented over a common time period for the case, for each alternative action considered (including the “status quo”/current state alternative).
iii. Are the assumptions and methods for assessing the proposal’s impacts clearly defined, understandable, and acceptable? Do not forget risk impacts!

iv. Does the business case include the non-financial costs and benefits?

v. Are the factors critical to the success of the proposal clearly defined?

vi. Are there critical success factors that can be managed? Is there a risk analysis that identifies and measures the relevant risks to the proposal?

vii. Are recommendations and conclusions based on a clear comparison of alternatives in terms of contributions to business objectives, problems solved, financial outcomes, and risks?

viii. Does the case clearly identify the estimated timeframes, costs, and implementation strategy required to successfully deliver the recommended solution?

ix. Does the case clearly express the consequences of failure to act on the recommended alternative?

e) Has the agency completed a risk assessment of the proposed IT Investment?

f) Has the agency thoroughly analyzed (and reengineered, if appropriate) agency business processes prior to proposing the automation of those processes through investments in technology?

g) Does the agency appear to have a plan for effective project management and intend to utilize appropriate system development lifecycle, project management, and quality assurance methodologies on the project?

h) Has the agency explored opportunities to partner with others on projects that can cross agency and program lines to leverage resources?

i) Does the proposed project align with State security architecture and standards?

j) Does the proposed project align with and support state data center standards and service offerings?

At this point in time, the review threshold for IT projects under the IT Investment Review and Approval Policy is any project that exceeds $150,000 or those projects that meet certain criteria contained within Guideline IV of the policy related to: Mainframe, Midrange, and Server hardware; IT security related hardware software and services; and non-ESRI based GIS Software.

The IT Investment Review and Approval Policy should be reviewed and revised as appropriate to address review requirements of SaaS solutions below and/or above the current review threshold of $150,000.


Appendix N: DAS State Data Center Exclusion Process/Policy

http://www.oregon.gov/das/sdc/docs/forms/SDC_Service_Scope_Exclusion_Form.doc
Appendix O: HB 2867

hb2867.en.pdf

Appendix P: Team A Candidate List of SaaS Domains

What are the domains the State should pursue?

Appendix Q: Cloud Security Alliance Guide V 2.1

csaguide.pdf

The Cloud Security Alliance (CSA) is a non-profit organization formed to promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.

The CSA is comprised of many subject matter experts from a wide variety disciplines, united in the following objectives:

- Promote a common level of understanding between the consumers and providers of cloud computing regarding the necessary security requirements and attestation of assurance.
- Promote independent research into best practices for cloud computing security.
- Launch awareness campaigns and educational programs on the appropriate uses of cloud computing and cloud security solutions.
- Create consensus lists of issues and guidance for cloud security assurance.

**Cloud Security Alliance Framework**

The Cloud Security Alliance (CSA) has recommended a simple framework to help evaluate initial cloud risks and inform security decisions. This framework includes:

- **Identify the Asset for Cloud Deployment:** The first step in evaluating risk for the cloud is to determine exactly what data or function is being considered for the cloud. This should include potential uses of the asset once it moves to the cloud to account for scope creep. Data and transaction volumes are often higher than expected. At the simplest, assets supported by the cloud fall into two general buckets:
  - Data
  - Applications/Functions/Processes
- **Evaluate each Asset by asking the following questions:**
  - How would we be harmed if the asset became widely public and widely distributed?
  - How would we be harmed if an employee of our cloud provider accessed the asset?
  - How would we be harmed if the process or function were manipulated by an outsider?
  - How would we be harmed if the process or function failed to provide expected results?
  - How would we be harmed if the information/data were unexpectedly changed?
  - How would we be harmed if the asset were unavailable for a period of time?
- **Map the Asset to potential Cloud deployment models including:**
  - Public
  - Private, internal/on-premises
  - Private, external (including dedicated or shared infrastructure)
  - Community; taking into account the hosting location, potential service provider, and identification of other community members
  - Hybrid. To effectively evaluate a potential hybrid deployment, you must have in mind at least a rough architecture of where components, functions, and data will reside
- **Evaluate potential cloud service models and providers**
- **Sketch out the potential data flow**
  - If you are evaluating a specific deployment option, map out the data flow between your organization, the cloud service, and any customers/other nodes. While most of these steps have been high-level, before making a final decision it's absolutely essential to understand whether, and how, data can move in and out of the cloud.
- **Make Conclusions**
  - You should now understand the importance of what you are considering moving to the cloud, your risk tolerance (at least at a high level), and which combinations of deployment and service models are acceptable. You'll also have a rough idea of potential exposure points for sensitive information and operations.

**National Institute of Standards and Technology (NIST)**

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Department of Commerce. NIST’s mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life. NIST’s role in cloud computing is to promote the effective and secure use of the technology within government and industry by providing technical guidance and promoting standards.

---

As cloud computing matures and becomes more ubiquitous; NIST and CSA will continue to develop and recommend security standards. Over time the state should identify and adopt those standards that are in alignment with or otherwise enhance the most current ESO standards for Enterprise Security. The state may want to consider developing an entirely new security domain specific to cloud computing as the model is further implemented into state government computing systems.

Appendix R: SaaS Procurement Process Map

Appendix S: Report from Karen Johnson, Department of Justice

Appendix T: Action Plan from Team B

Appendix U: SaaS Solution Selection Criteria

<table>
<thead>
<tr>
<th>No.</th>
<th>SaaS Solution Selection Criteria</th>
<th>Horizontal applications\textsuperscript{10}</th>
<th>Vertical applications\textsuperscript{11}</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Avoid duplication - the State should be using a single instance of the software.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Enable business needs – the selected solutions has to directly address and help achieve specific business needs of the agencies and state as an enterprise.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Vendor stability / maturity – the selected vendor needs to have a stable financial situation and experience in delivering the solution; its track record needs to prove the maturity and stability.</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

\textsuperscript{10} A horizontal application is a software package designed to be used by many different kinds of organizations and individual users. In terms of the SaaS strategy, horizontal applications refer to applications that will be used by all/multiple agencies.

\textsuperscript{11} A vertical application is a software package designed to be used by a single market. In terms of the SaaS strategy, vertical application refer to applications that will be used by single agencies for particular needs specific to the area of business.
<table>
<thead>
<tr>
<th></th>
<th>Vendor capacity / Disaster recovery – the selected vendor needs to have the capacity to satisfy the State needs for a large number of end-users.</th>
<th></th>
<th>Yes</th>
<th>Yes</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td><strong>Interoperability</strong> – the new SaaS solution needs to integrate well with the diverse applications and systems the State agencies use.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td><strong>Cost and time of implementation</strong> – the benefits of implementation need to outweigh the effort - financial effort as well as other resources required.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>7</td>
<td><strong>Scalability</strong> – the vendor needs to be able to deliver high quality solution to an increased number of end users over time.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td><strong>Security and privacy</strong> – the vendor needs to be able to address the security and privacy requirements of the agencies.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td><strong>Tiered pricing/service offerings</strong> – because of the large number of end-user inside the agencies, the State needs to look at opportunities for achieving economies of scale.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td><strong>Exiting</strong> – before acquiring a solution the State needs to develop an exiting strategy: this refers to vendor change or even changing back to hosted solutions.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>11</td>
<td><strong>Functionality</strong> – the basic attributes of the solution needs to be satisfy specific requirements the agencies set.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td><strong>Enterprise authority</strong> – for horizontal solutions that will be implemented state-wide, the State needs to assign an executive team in charge of high-level decision making for the new solution.</td>
<td></td>
<td>Yes</td>
<td>Not applicable</td>
</tr>
<tr>
<td>13</td>
<td><strong>Stakeholder group</strong> – for horizontal application the State needs to select a multi-agency team in charge of dealing with any issues related to the new solution.</td>
<td></td>
<td>Yes</td>
<td>Not applicable</td>
</tr>
<tr>
<td>14</td>
<td><strong>Short and long term cost</strong> – when acquiring a new solution the TCO (Total Cost of Ownership) needs to be calculated for short and long-term and the cost effectiveness needs to be addressed.</td>
<td></td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>