OSCIO statewide policy

DAS DEPARTMENT OF ADMINISTRATIVE SERVICES

NUMBER	SUPERSEDES
107-004-150	107-004-150 | 7/18/2016

STATEWIDE POLICY

EFFECTIVE DATE	DATE OF LAST REVIEW
5/1/2019	**5/25/2019**

DIVISION	REFERENCE/AUTHORITY
Office of the State Chief Information Officer	ORS 276A.206 Cloud and Hosted Systems Procedure: 107-004-150_PR.
POLICY OWNER	
Enterprise IT Governance	
SUBJECT	**APPROVED SIGNATURE**
Cloud and Hosted Systems	**Terrence Woods, State Chief Information Officer** ***(Signature on file with DAS Business Services)***

PURPOSE

This policy establishes standards to ensure that state agencies:

- Appropriately analyze and document the benefits, costs, and risks to the state before contracting for a Cloud or Hosted Service.
- Assess the readiness of a Cloud or Hosted Service Provider to deliver a solution that meets the state's requirements.
- Conduct planning to ensure that state information and financial assets are appropriately protected when adopting a Cloud or Hosted Service.

APPLICABILITY

This policy applies to all state agencies as defined in ORS 276A.230, and includes any board, commission, department, division, or office within the Oregon Executive Branch. The following agencies and boards are excluded:

- Secretary of State.
- State Treasurer.
- The Attorney General, but only with respect to its authority under ORS 276A.303 over information systems security in the Department of Justice.
- Oregon State Lottery.
- State Board of Higher Education or any public university listed in ORS 352.002.

FORM(S), EXHIBIT(S) & INSTRUCTIONS

These governing statutes, policies and rules must be reviewed prior to contracting for a Cloud or Hosted Service:

- Information Technology Investment Oversight Policy: 107-004-130.
- Information Security Policy: 107-004-052.
- Information Security Incident Response Policy: 107-004-120.
- Information Asset Classification Policy: 107-004-050.
- Cloud and Hosted Systems Procedure: 107-004-150_PR.
- ORS 291.047; 192.005; 192.311 to 192.478; and 279A.157.

- ORS 165.800; and 646A.600 to 646A.628.
- ORS 276A.300; and OAR 125-800-0005 to 125-800-0020.
- SB 1538 (Chapter 110, 2016 Laws).

Exhibit A attached, Cloud and Hosted Systems Workbook Guide supports the Cloud or Hosted Service purchasing process. Fillable form available at: https://www.oregon.gov/das/Policies/107-004-150_PR_Attachment.docx.

DEFINITIONS

- "Cloud or Hosted Service": an Internet-based computing solution that provides shared processing resources, applications and access data on demand, made available to state agencies through various contracting models.
- "Cloud or Hosted Service Provider" or simply "Provider": the entity providing a Cloud or Hosted Service.
- "Service Contract": all of the documents that comprise a contract for a Cloud or Hosted Service between a Cloud or Hosted Service Provider and an agency.
- "Information Asset Classification Level": the classification of information by value, criticality, sensitivity, and legal implications to protect the information through its life cycle. Classification Levels are defined in DAS Policy 107-004-050 and referred to in statewide information security standards.
- "Public Record": has the meanings established in ORS 192.005 and ORS 192.311. In general it refers to information that is prepared, owned, used or retained by a state agency; relates to an activity, transaction or function of a state agency; and is necessary to satisfy the fiscal, legal, administrative or historical policies, requirements or needs of the state agency. It includes any writing that contains information relating to the conduct of the public's business, including but not limited to court records, mortgages, and deed records, prepared, owned, used or retained by a public body regardless of physical form or characteristics.

EXCLUSIONS AND SPECIAL EXCEPTIONS

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

GENERAL INFORMATION

Strategic Considerations:

(1) The choice of a Cloud or Hosted System over an agency-managed system can have substantial, long-term impact on agency and enterprise capabilities, business processes and investments. Agencies should carefully consider the strategic implications of this sourcing decision, including how it will affect the organizational capabilities of the agency; whether the service is likely to serve the agency's long-term goals, and how the service and data will integrate with other state services and data to support service delivery and ongoing innovation.

(2) Cloud or Hosted Systems and Services may present limitations or challenges for integrating data or services with other agency, state or partner data or services. Agencies should consider how future business needs may create demands for data and service integration, and how these demands will be met. Contractual terms may be helpful in ensuring that data and services are available for integration, for example through documented and supported Application Programming Interfaces (APIs).

Requirements:

(1) The selection and use of Cloud or Hosted Systems and Services must comply with all applicable laws, policies, procedures and standards including without limitation: privacy laws and regulations, statewide and agency-specific IT security policies and standards, internal audit controls, risk management standards, records management standards, and applicable DAS policies and procedures.

(2) Before contracting for a Cloud or Hosted Service, the agency must complete the planning and preparation necessary to appropriately manage the associated risks. Planning should be started as soon as a Cloud or Hosted Service is considered, and must be carried out with diligence and rigor appropriate to the size, business impact and risk of the proposed solution. Details of required documentation and timing are provided in the Cloud and Hosted Systems Procedure.

Use the Cloud and Hosted Systems Workbook (form), published by the State CIO, to document the results of this planning. The completed, signed workbook must be retained as part of the procurement file and submitted with supporting documentation as required by this policy and its associated procedure when seeking approval from the State CIO. When required, such approval must be obtained before continuing with the initiative.

The following risk areas must be addressed:

(a) Confidentiality, availability and integrity: Agencies must develop information security plans and Service Contract terms to protect information to all applicable standards. Among other guidance, the following apply to every information technology initiative:

- Information Security Policy: 107-004-052, which requires agencies to develop and implement information security plans, policies and procedures to protect their information.
- Statewide Information Security Standards, which the Enterprise Security Office (ESO) publishes and maintains as minimum standards for protecting information.

(b) Business continuity and disaster recovery: Agencies must document their business continuity (BC) and disaster recovery (DR) needs, and must develop plans and Service Contract terms to meet those needs. The impact of this IT investment must be reflected in the agency's BC/DR plan.

(c) Exit planning: Agencies must develop plans for both anticipated exit from the Cloud or Hosted Service (such as at the end of the Service Contract term) and unanticipated exit (in case the Provider becomes unwilling or unable to provide the Service).

(d) Service management: Agencies must document their required service levels and metrics and ensure that they are appropriately represented in the Service Contract.

(e) Incident management: ESO (Security Operation Center) will assist agencies in the development of security incident response plans and Service Contract terms that meet their needs for incident monitoring, notification and response. At a minimum, the following applies to every Cloud or Hosted Service:

- Information Security Incident Response Policy: 107-004-120 which requires agencies to establish capabilities to respond to information security incidents and requires the timely reporting of certain incidents.

(f) Data ownership and rights: Agencies must document their requirements in regards to data and metadata ownership and rights and ensure that those rights are appropriately secured and allocated in the Service Contract.

(g) Data retention and destruction: Agencies must document the retention and destruction schedules that apply to the information stored in the Cloud or Hosted System, and the required ability to retrieve records as needed. Agencies must develop plans and Service Contract terms to meet these needs and to ensure the ability to comply with Oregon Public Records laws and with all other applicable federal and state statutes, rules, and policies.

- The State Archivist is responsible for the management of public records from creation until final disposition. Agencies are required to develop policies for public records management that define the use, retention and ownership of public records and to obtain approval of those policies from the State Archivist.

(h) Audits and Controls: Agencies must determine how they will ascertain that the Provider has appropriate controls in place to meet agency needs as described in sections A-G above, and to comply with applicable legal, regulatory, and contractual commitments. Each Service Contract must include terms ensuring that appropriate audits are carried out and reports are made available, and that Provider cooperation is appropriately secured for audits by or on behalf of the agency.

(3) If the Cloud or Hosted Service meets or exceeds any of the triggering risk thresholds described below, the agency must obtain approval from the State CIO before contracting for the Cloud or Hosted Service. This approval is required in addition to any other oversight that the State CIO may impose, such as through the Stage Gate or Non-Stage Gate oversight processes. Agencies must submit proposals for oversight if any one or more of the following risk thresholds apply to the proposed Cloud or Hosted System or Service:

- It will store, process, or transmit data of Information Asset Classification Level 3 (Restricted; reference Policy 107-004-050) or higher, or information for which special protection standards apply by law or contract.
- It will be the authoritative source for information that is difficult, expensive, or infeasible to replace or recreate.
- A sustained interruption of the Service would have a significant impact on agency operations and/or those served by the agency.

(4) Agencies must also follow the IT Investment Oversight Policy: 107-004-130.

(5) Service Contracts must include terms and conditions required by the Attorney General in order for the contract to be approved for legal sufficiency according to ORS 291.047. Service Contracts must use available forms and templates developed by DAS and the Department of Justice according to ORS 279A.

(6) Service Contracts must require the contractor to carry insurance appropriate for the proposed transaction, as informed by the tools and guidance provided by DAS Risk Management.

OREGON | Office of the State
Chief Information Officer

Cloud and Hosted Systems Workbook Guide

Exhibit A

Version 2.0
Date: 25 APRIL 2019
For the latest version, visit:
https://www.oregon.gov/das/OSCIO/Pages/OSCIO-templates-and-forms.aspx

For additional information, please contact**:**
Your Senior IT Portfolio Manager, or
ITinvestment.Review@oregon.gov

Enterprise IT Governance office

Table of Contents

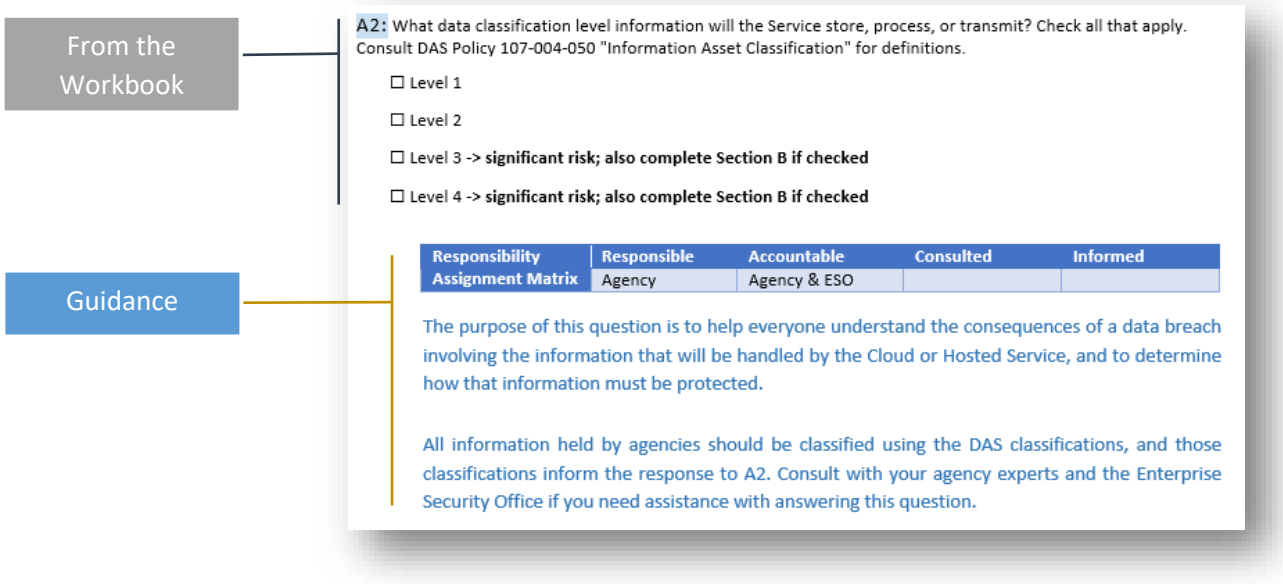
INTRODUCTION

This guide is intended to support agencies in complying with the state's Cloud and Hosted Systems Policy (DAS policy 107-004-150), in particular with their completion of the Workbook. It is a living document maintained by the Enterprise IT Governance team (EITG) in the Office of the State CIO (OSCIO). Please note the version and date in the footer and compare against the latest version online to be sure that you are working with the most current guide. EITG welcomes your questions and suggestions, which we will use to continuously improve this guide. Communications about this guide can be addressed to your agency's senior IT portfolio manager or sent to ITInvestment.Review@oregon.gov.

HOW TO USE THIS GUIDE

Throughout this guide, text that is blue and indented is the text of the guide. Text in black, non-indented is from the Cloud and Hosted Systems Workbook. Capitalized terms in this guide refer to the definitions in the Cloud and Hosted Systems Policy.

This guide follows the structure of the Workbook and provides specific guidance on the purpose of each question, explanation of the terms used, and instructions for how to determine and provide your answer. This includes a *Responsibility Assignment Matrix* to show the commitment of our Enterprise Security Office (ESO) and EITG teams to collaborate and help complete the Workbook. Guide sections are immediately below the Workbook text that they relate to, as demonstrated below:



Definitions

- ***Cloud or Hosted Service*** means an Internet-based computing solution that provides shared processing resources, applications and access to data on demand.
- ***Cloud or Hosted Service Provider*** or simply ***Provider*** is the entity providing a Cloud or Hosted Service.
- ***Service Contract*** means the sum total of all of the documents that comprise a contract between a Cloud or Hosted Service Provider and an agency for a Cloud or Hosted Service.
- ***Information Asset Classification Level*** is the classification of information by value, criticality, sensitivity, and legal implications to protect the information through its life cycle. Classification Levels are defined in DAS Policy 107-004-050 and referred to in statewide information security standards.
- ***Public Record*** has the meanings established in ORS 192.005 and ORS 192.311. In general it refers to information that is prepared, owned, used or retained by a state agency or political subdivision; relates to an activity, transaction or function of a state agency or political subdivision; and is necessary to satisfy the fiscal, legal, administrative or historical policies, requirements or needs of the state agency or political subdivision. It includes any writing that contains information relating to the conduct of the public's business, including but not limited to court records, mortgages, and deed records, prepared, owned, used or retained by a public body regardless of physical form or characteristics.
- ***Low Risk*** means that agency operations can continue and services will provided with negligent impact to mission of the agency. Alternative way of providing the services are available during the interruption of the contracted service.
- ***Significant Risk*** means that agency operations will be degraded with significant impact to the mission of the agency. No alternative way of providing the services during the interruption.
- ***Incidents*** here refers broadly to information security incidents, which may include or a breach or potential breach of security or privacy, or a failure to comply with the vendor's confidentiality obligations.

GENERAL INFORMATION

The Workbook does not stand alone; it implements the Cloud and Hosted Systems Policy. Agencies should read and refer to the Policy while working to comply with it. The Workbook is simply a way of documenting compliance.

The Enterprise Security Office (ESO) will provide direct assistance in completing the security sections of the Workbook in collaboration with the agency. Contact ESO early in the process through ESO.info@oregon.gov.

WORK REDUCTION AND REUSABILITY

Many contractual and Requests for Proposal (RFP) requirements are similar over time and across agencies, vendors, and systems. In order to facilitate approvals, OSCIO is working to support and promote reusability in several ways, namely: boilerplate language, re-use of completed workbooks, and fast-lane renewals.

OSCIO-APPROVED BOILERPLATE LANGUAGE

OSCIO is collaborating with the Department of Justice (DOJ) and DAS Procurement Services (PS) to craft terms that agencies can use in contracts and RFPs. The first such offering is under development at the time of writing this Guide, but is not yet ready for release. OSCIO envisions an approach in which an agency can follow a simple decision tree in order to identify suitable boilerplate language from what will be provided as a result of the work completed by DAS PS and DOJ.

RE-USE OF COMPLETED WORKBOOKS

Along with the rollout of this 2019 policy revision, OSCIO is committing to maintain a repository of completed workbooks which can form the basis for re-use. That work is ongoing and will be documented here as it evolves.

FAST-LANE RENEWALS

This 2019 revision creates a new process to facilitate contract renewals if there were no substantive changes to the submitted workbook since it was last approved by OSCIO under the Cloud and Hosted Systems Policy. This is documented in section C of the workbook. If an existing contract that is up for renewal has not been subject to OSCIO review and approval under the Cloud and Hosted Systems Policy, it does not qualify for a fast-lane renewal. See “First-time review of existing contracts” below.

FIRST-TIME REVIEW OF EXISTING CONTRACTS

When an agency plans to renew or amend a Service Contract for a Cloud or Hosted Service or Service, and the Service Contract has not previously been approved by OSCIO under the Cloud and Hosted Systems Policy, the agency should complete and submit the Workbook as is required for a new Service.

The *Section A: Risk Determination* section must be completed to determine if OSCIO review is required. If required as a result of filling out Section A, then *Section B Sub-Section 1: Requirements* of the Workbook (“Requirements”) must be completed and submitted for OSCIO approval prior to negotiating a finalized contract for renewal.

In many cases, older contracts are lacking important terms and controls, and renewal is an opportunity to address the risk associated with such contracts. If required, *Section B: Sub-Section 2: Contract and related planning* ("Contract and related planning") must be completed and submitted for OSCIO approval prior to executing the renewal.

Agencies should budget sufficient time and resources to discover and address risks in existing contracts during the renewal process.

QUESTION-BY-QUESTION GUIDANCE

The following pages contain section-by-section guidance to help agencies complete the workbook.

(Remainder of Page Intentionally Left Blank)

GUIDANCE ON SECTION A: RISK FACTORS DETERMINATION

When is Section A of the Workbook required? Always (except for renewals of investments previously approved under the Cloud and Hosted Systems Policy or its predecessor the Cloud Computing Policy) where a cloud workbook was completed and approved.

Purpose of Section A of the Workbook: This section documents the risk posture of the proposed or ongoing investment, which may allow the agency to proceed with low-risk investments easily and quickly, and determines if any risk thresholds are met that will require completion of Sections B, Sub-Section 1 and 2 of the workbook as needed.

If any (one or more) answer in this section directs the agency to "also complete Section B, Subsections 1 and 2 of the workbook" then the investment is considered "significant risk".

The agency is then required to complete section B, Subsections 1 and 2 of the Workbook according to the instructions in the Policy and Workbook, as supported by this guide.

If no answer in this section directs the agency to "also complete Section B" then the investment is considered "low risk". In that case the agency may proceed with the investment and is not required to complete sections 2 or 3 of the Workbook.

Is the agency required to complete Section A of the cloud Workbook? Yes, for every IT investment that may include a cloud or hosted component, as defined in the Cloud and Hosted Systems Policy.

At what point in the IT investment initiation process must the agency complete the Section A of the cloud Workbook? As early as possible. This section must be completed before releasing a procurement document or selecting a solution. Ideally this section should be completed as soon as the agency believes that a cloud solution may be considered.

Is OSCIO submission/approval required for Section A of the cloud Workbook? No, agencies are not required to obtain OSCIO approval for this section when the assessment determines that risk is low. The agency must keep a completed, signed copy of this section with the procurement file. It must also be submitted to OSCIO for documentation along with relevant facts related to the risk determination.

The IT service/product name, agency name, division, and contact info on this form should match that what was used on any ITI and associated documents. It is strongly preferred that the service/product name remain unchanged for the duration of service/product planning, implementation and oversight, since much confusion can develop from inconsistency in naming.

A1: What is the main function of the proposed Cloud or Hosted Service and how will it be used to support one or more business functions? Briefly describe and include the number of records anticipated and how that number is anticipated to grow over time; the number of users; and the anticipated cost. A completed IT Investment form with the same information may be attached instead, if available.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency	Agency	SIPM	ESO

The purpose of this question is to provide a context for understanding the answers provided in subsequent sections of the workbook. This section does not need to justify the investment, but rather should briefly explain its purpose and the IT and business context for the service/product.

Do not duplicate work. If an ITI form is required according to the IT Investment Oversight Policy (DAS policy 107-004-130), you should just complete that form and attach it instead of answering this question (as long as it includes all the information requested). If you do this please reference the ITI in the Workbook e.g., "See attached ITI form."

Note: While the Cloud and Hosted Systems Workbook does not require a discussion of alternatives, the ITI does. The guidance on the current (9/2018) ITI form states: "Include high level business opportunity, proposed solution, alternatives to be considered, and anticipated impacts".

A2: What data classification level information will the Service store, process, or transmit? Check all that apply. Consult DAS Policy 107-004-050 "Information Asset Classification" for definitions.

☐ Level 1

☐ Level 2

☐ Level 3 **-> significant risk; also complete Section B if checked**

☐ Level 4 **-> significant risk; also complete Section B if checked**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency	Agency & ESO		

The purpose of this question is to help everyone understand the consequences of a data breach involving the information that will be handled by the Cloud or Hosted Service, and to determine how that information must be protected.

All information held by agencies should be classified using the DAS classifications, and those classifications inform the response to A2. Consult with your agency experts and the Enterprise Security Office if you need assistance with answering this question.

A3: Will the proposed Service store, process, or transmit data that must be protected according to the following specialized rules or standards? Check all that apply.

If any items below are checked, the investment has significant risk; also complete Section B

☐ HIPAA (Protected Health Information)

☐ CJIS (Criminal Justice Information)

☐ IRS Publication 1075 (Federal Tax Information)

☐ FERPA (certain education records)

☐ PCI (payment card data)

☐ SSA (Social Security Administration)

☐ Other, please identify the rule or standard:

☐ FISMA (Federal Information Security Modernization Act)

☐ MARS-E (Minimum Acceptable Risk Standards for Exchanges)

☐ OCITPA (Oregon Consumer Identity Theft Protection Act)

☐ No checkboxes apply

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency	Agency	ESO	

Similar to the preceding Question A2, the purpose of Question A3 is to help everyone understand the consequences of any data breach involving the information that will be handled by the Cloud or Hosted Service,, and to determine how that information must be protected.

Agencies should be aware of all specialized rules and standards that apply to the protection of their data. Consult with your agency experts and the Enterprise Security Office if you need assistance with answering this question.

A4: Will the Service be the authoritative source for any business-critical information that would be difficult, expensive, or infeasible to recreate? Check one.

☐ No (check this box if data in the Service is a copy of another authoritative source; if it could be easily recreated; or if loss or corruption of the data would have no significant consequences)

☐ Yes (check this box if loss or corruption of the data would create significant expense, risk, or impact; or it is the system of record) **-> significant risk; also complete Section B workbook if checked**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency	Agency	SIPM, ESO	

The purpose of this question is to help us understand the consequences of information that will be handled by the Cloud or Hosted Service being corrupted or lost. This takes into account two separate concerns.

First, **is the system in question the authoritative, go-to source for the information**? Another term

for this is the "system of record" or "source of record". The agency may designate any copy of its data as the "source of record".

Second, **is the data in question critical to your business**? Data could be critical because it is operationally critical, because it is subject to retention rules, or for other reasons.

You may answer "no" to this question if the Cloud or Hosted Service is not your agency's dedicated system of record. For example, if your processes are such that copies of all data are kept up-to-date on servers at the State Data Center, and that because of this your agency would face minimal or zero data loss if the vendor's system were to become suddenly and permanently unavailable, then you could reasonably answer "no" to this question.

You may also answer "no" to this question if the data in question could be easily recreated. For example if you use the service to process data that is drawn from servers at the State Data Center, and it would be easy to repeat the processing if the service were lost, you could reasonably answer "no" to this question.

A5: Would a sustained interruption of the Service have a significant impact to Oregonians and also to the agency, the State, and partner organizations? Check one.

☐ Minor impact. Check this box if agency operations would be able to continue without significant impact to Oregonians, the agency, the state, or partner organizations.

☐ Significant impact. Check this box if an interruption would have anything more than a minor impact**. -> significant risk; also complete Section B workbook if checked**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency	Agency		SIPM, ESO

The purpose of this question is to help everyone understand the consequences for key stakeholders and users if the service itself were lost or unavailable for a protracted period. This question focuses on "sustained" interruptions. Short interruptions are typical in many services and are most usually managed according to a service-level agreement (SLA) with the vendor. This question is concerned with interruptions that would substantially violate the SLA and would not be promptly cured.

There is no one-size-fits-all time period appropriate to every service. In addition, the consequences of a sustained outage will depend on the agency's business continuity needs and plans.

Even if the data are protected because up-to-date copies are kept at the State Data Center, there may be adverse consequences if the service were to become unavailable.

The thing to focus on here is the impact. If you normally count on the service being available 99.9% of the time during business hours and it is down for several days, what would the impact be? For example, for some systems, such as a survey tool that is used for periodic, non-essential data gathering the impact might be minor. For a case management system that must be consulted and updated during every client interaction, impact might be significant.

A6: Will the Cloud or Hosted Service and all associated data reside entirely in the United States?

☐ Yes

☐ No **-> significant risk; consult with OSCIO before proceeding to complete Section B workbook if checked**

☐ Not known **-> significant risk; consult with OSCIO before proceeding and complete Section B workbook if checked**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency	Agency		SIPM, ESO

In general, the State requires that data under State stewardship **reside in the USA**. Any exception to this would need to be explicitly approved.

AGENCY CONCLUSION:

☐ Low Risk: check only if no "significant risk" box above is checked.

☐ Significant Risk: check if any one or more "significant risk" boxes above are checked.

If the solution is found to be "low risk", file this completed, signed, and dated section with the procurement documents. Submit a copy of the same to OSCIO for record keeping, no approval is required.

If the solution is found to involve "significant risk", then Section B must be completed and submitted, in partnership with ESO, according to the directions in the Workbook, Policy, and Procedure.

If the results of completed Section A indicates a potential security risk and the services needed do need requirements for potential RFP then Section B1 is completed and submitted with ESO and agency sign off. Then further interaction is needed between the agency and ESO to complete Section B2 and inform the oversight analyst to complete the checklist for the next endorsement that could be provided to the agency to proceed.

APPROVING BUSINESS OWNER SIGNATURE

First name Last name Title Click here to enter a date

X

APPROVING TECHNOLOGY MANAGER SIGNATURE

First name Last name Title Click here to enter a date

X

ESO SIGNATURE

First name Last name Title Click here to enter a date

X

The form must be signed by managers who are authorized to make risk acceptance decisions for the business. The business owner should be a senior manager, director, or agency director who is accountable for both the performance and the risks regarding the relevant system and data. The technology manager should be the CIO, deputy CIO, or other executive in charge of agency IT. If these two roles fall to the same individual, one should be escalated to senior management. An ESO representative will also verify/validate and sign the information presented in this form.

The agency may be called upon to produce the signed Risk Determination section in the event of an audit, incident, or inquiry. For low risk service/products completing this document accurately is a requirement of accepting delegated responsibility, from OSCIO, for managing the associated risk and proceeding without oversight.

GUIDANCE ON SECTION B SUB-SECTION 1: REQUIREMENTS

Required when the Section A of the workbook identifies significant risk

Purpose of this section: To document that the solution selection process is informed by clearly understood business needs (also known as requirements). Clearly documenting business needs is an important component of managing the risk of an investment – when requirements are not clear and precise enough, agencies may discover late in negotiations that the vendor is unable to meet some necessary condition, or that meeting it will substantially increase cost and/or project duration. This is a common issue, and it can be mitigated by the advance planning required by the Cloud and Hosted Systems Policy.

Is the agency required to complete this section? The agency must complete this section if any answer in Section A indicates that the "Section B" must be used or if directed to do so by the assigned OSCIO Oversight Analyst.

When must the agency complete this section? This section must be completed (and approved, if OSCIO approval is required) before releasing a procurement document or selecting a solution. The information in this section should inform the requirements statements in the procurement documents.

Is OSCIO submission and/or approval required?

Yes, if the service/product is under OSCIO Stage Gate or Non-Stage Gate oversight per the IT Investment Policy (107-004-130). Submit this section with a copy of the Section A of the Workbook and obtain approval before proceeding.

Yes, if OSCIO approval is required for the procurement. Submit this section with a copy of the Section A of the Workbook and obtain approval before proceeding.

Otherwise, no; OSCIO approval is not required at this stage. The agency must keep a completed, signed copy of this section with the procurement file and submit a copy of the same to OSCIO for record keeping.

For each question in this section:

Note your requirements and where they are recorded. If you have formal requirements documents, cite specific sections of those documents. Where available, OSCIO-approved boilerplate language that is suitable to your specific use case can be used. Cited documents should be attached.

B1-1: What controls does the agency expect the cloud and hosted systems vendor to have in place to protect state data against unauthorized access ("confidentiality"), loss ("availability"), and corruption ("integrity")? In addition, the vendor must agree to comply with State standards, rules, laws, and policies, as they are updated from time to time. The current state standards are available at: https://www.oregon.gov/das/OSCIO/Pages/Security.aspx

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

The purpose of this question is to validate that the agency has identified and clearly documented requirements for how the vendor must protect information accessible to the cloud and hosted system. State standards provide a minimum level.

The answer to this question should inform the related answers to Questions 1, 2, 3 and 7 in Section B of the Workbook.

B1-2: What are your business requirements for availability? This answer should represent the tolerance of supported business processes to planned and unplanned outages. Note acceptable downtime, planned and unplanned, during regular business hours and off hours.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

The purpose of this question is to validate that the agency has identified and clearly documented availability requirements for the cloud and hosted system.

The most common problem here is that agencies simply adopt whatever availability guarantees the vendor offers. Unsurprisingly, this tends to benefit the vendor and it is not a recommended practice. Your answer should be informed by considering actual impact on your business. Lowballing this number could result in the agency agreeing to unacceptably low service levels; for example, if monthly uptime of 99% (measured 24/7) is promised, the system could be down for almost a full business day (7.2 hours in a 30-day month). Is it acceptable to your business if this happens every month? In contrast, highballing this number could create unnecessary expense. “Five 9s” availability (99.999%) reduces expected downtime to only about 5 minutes per year but can be very expensive.

The answer to this question should inform the related answers to Question 4 in Section B Subsection 2 of the Workbook.

B1-3: Document minimum requirements that the vendor must meet in order to comply with agency incident management needs, including the statewide security incident response policy and plan. State security incident response standards are available at: https://www.oregon.gov/das/OSCIO/Pages/SecurityResponse.aspx

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

The purpose of this question is to validate that the agency has identified and clearly documented minimum incident response requirements for the cloud and hosted system. At a minimum, agencies must be able to meet state standards, which require notification of a security incident within 24 hours.

The answer to this question should inform the related answers to Question 5 in Section B, Subsection 2 of the Workbook.

B1-4: Document agency requirements to maintain ownership of data to include retention, destruction requirements as needed and restrict usage by the vendor. Be sure to address metadata and derived data.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

We ask these questions to validate that the agency has identified and clearly documented requirements around rights to data and metadata that are accessible within the cloud and hosted system. "Metadata" means information about the data, such as the number of records, or how frequently they are accessed. The agency may also wish to define and control rights to summarized, aggregated, or derived data (such as averages or geographical distribution) even if those are less sensitive than raw data.

The answer to this question should inform the related answers to Question 6 in Section B, Subsection 2 of the Workbook.

B1-5: How will the agency document and verify (audit) that the vendor has appropriate controls in place to deliver on the confidentiality, availability, and integrity commitments documented in this worksheet and the Service Contract? Vendors must typically agree to carry out regular third-party audits with specified scope and standards, and must agree to promptly provide such audit results to the agency.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency	SIPM	

The purpose of this question is to validate that the agency has identified and clearly documented audit requirements. Audits are undertaken to provide the agency with a regular assessment of whether the vendor is able to meet its contractual commitments related to security controls.

While there is no single audit standard that is uniformly required, the state frequently accepts a SOC2 Type 2 audit covering all five Trust Services Criteria. Other types of audits or certifications, such as FedRAMP, may also be acceptable. Agencies should work with OSCIO throughout the process to ensure that audit standards are acceptable.

A common mistake in this area is for the vendor to provide an audit from a third-party hosting company, but not to provide their own audit of its application/system that is hosted there. If the vendor is operationally involved in managing the system, their operations also need to be audited.

The contract should require the vendor to promptly and fully share the results of all security audits, which may be done under nondisclosure terms.

The answer to this question should inform the related answers to Question 8 in Section B Subsection 2 of the Workbook.

APPROVING BUSINESS OWNER SIGNATURE

First name Last name Title Click here to enter a date

X

APPROVING TECHNOLOGY MANAGER SIGNATURE

First name Last name Title Click here to enter a date

X

ESO SIGNATURE

First name Last name Title Click here to enter a date

X

See the guide section for the Section A of the Workbook, above, for information about who should sign. See the notes at the top of this section in order to determine whether the agency must submit this section for OSCIO approval before proceeding.

GUIDANCE ON SECTION B SUB-SECTION 2: CONTRACT AND RELATED PLANNING

Required when the short workbook identifies significant risk

Purpose of this section: To validate that the implementation plan, including the vendor contract and also agency decisions, processes, and controls are designed to appropriately manage any risks identified.

Is the agency required to complete this section? The agency must complete this section if any answer in Section A indicates that Sections A and B must be completed or if directed to do so by OSCIO.

When must the agency complete this section? This section must be completed before the agency obligates the State to acquire/implement a particular solution, i.e. before signing a contract, purchase order, or other binding document.

Is OSCIO approval required? Yes. Whenever the agency is required to complete this section, OSCIO approval must be obtained before executing a contract, purchase order, or other binding document. Submit together with Section A and Section B of the Workbook, unless they were previously submitted and approved.

For each question in this section:

Provide supporting documentation as needed, citing specific contract sections. Where available, OSCIO-approved boilerplate language that is suitable to your specific use case can be used. Cited documents must be submitted along with the signed workbook.

B2-1: Document how the Service Contract ensures appropriate protection of the data against unauthorized access ("confidentiality"), loss ("availability"), and corruption ("integrity").

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

The purpose of this question is to validate that the vendor is contractually bound to provide appropriate protection for the data. This includes both the specification of appropriate protection standards and the commitment from the vendor to meet them.

B2-2: Document how the Service Contract requires the vendor to maintain disaster recovery systems and processes sufficient to protect agency interests.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency	SIPM	

The purpose of this question to validate that the vendor is contractually bound to meet agency needs for resiliency and recoverability of the data and the service. Modern architectures have expanded on the number of ways this can be achieved—for example using geo-redundant high availability solutions may reduce the need for tape backups. Any strategy that meets agency needs is acceptable to OSCIO.

B2-3: Does the agency have strategies for both planned and unplanned exit from the Cloud or Hosted Service? Briefly describe them. Consider plans for data transfer at exit. Document how the Service Contract supports the agency's exit strategy, including how it codifies vendor and agency responsibilities during exit planning and during planned or unplanned exit.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency	SIPM	

The purpose of this question is to validate that the agency has appropriate planning and contract terms in place to support planned or unplanned service termination. In many cases the agency need for the data and service will last longer than the relationship with one vendor. Planning in advance for this exit is critical.

Where necessary, the contract should include provisions that apply at exit to support graceful transition. This avoids the need to carry out exit negotiations under duress. DOJ and OSCIO can assist agencies with boilerplate language that supports planned transitions.

Over and above contract language, this area of planning typically involves significant effort by the agency. Often such plans are based on access to data files. The likelihood of easy transition is much higher when this is built into both the contract and operational planning. Planning might for example include:

- a contractual agreement to regularly test data transfer as part of a project and during the maintenance and operations phase of the investment;
- a testing plan that indicates how the agency and vendor will test and how they will demonstrate that the test results in fully usable copies of the data, suitable to support ongoing agency needs;
- the assignment of agency resources to carry out this periodic testing as part of their regular job duties; and a mechanism to document and continuously improve based on the results of testing.

B2-4: Document how the Service Contract binds the vendor to deliver required service levels.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency	Agency	SIPM	ESO

The purpose of this question is to validate that the agency has appropriate contract terms in place to hold the vendor accountable for delivering required service levels. These are typically recorded in a "service level agreement" or SLA. Service levels should meaningfully address agency needs and should, wherever possible, be created so as to address the end-user experience. The SLA or supporting documentation should also describe the responsibility of the vendor and the agency to communicate about and respond to reports of service issues.

B2-5: Document how the IT incident, security incident and change management processes and the responsibilities of each party are spelled out in the Service Contract.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

The purpose of this question is to validate that appropriate contract terms are in place so that the state can to respond to any incidents. Contract terms may include the vendor's obligation to promptly report the incident, to fully and promptly share all available information about the incident, and to honor the state's needs for communicating publicly or privately about the incident. Some vendor contracts seek to limit the ability of their clients to communicate freely about security incidents, and agreeing with this may not always be in the best interest of the state.

B2-6: Document how the Service Contract defines data ownership and rights for the vendor and the agency. Be sure to address metadata.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency	SIPM	

The purpose of this question is to validate that contract adequately describes data ownership, rights, and responsibilities. See Section B of the Workbook, Question 4, requests similar contractual obligations to be addressed.

B2-7: Document how the Service Contract captures appropriate retention and destruction commitments from the vendor, including (as necessary) a commitment to certify destruction meeting specified standards.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency	SIPM	

The purpose of this question is to validate that the agency's engagement with a cloud and hosted system provider has the ability to meet state data retention and destruction requirements. Destruction is typically more difficult to plan for, carry out, and certify than retention. The agency should be clear on whether it will need to purge specific records or groups of records, and how they will ensure that those records will be effectively deleted by the vendor. It can be helpful to understand the backup cycle and know whether records are ever fully deleted or will remain archived in some medium. A common mistake in this area is to refer to standards for media sanitization in ways that they are not applicable. The NIST standard generally cited (NIST SP800-

88) only refers to complete sanitization of the medium (such as a hard drive) and does not provide standards for deleting particular records such as a single file or database row. This is great when it applies, but unhelpful when it does not.

B2-8: Document how the Service Contract requires the vendor to perform, cause to be performed by a third party, and/or cooperate with audits. Document what audit results must be provided to the agency. Note what standards of audits apply (for example, SOC 2 Type 2), how frequently audits must be performed, whether the state will obtain complete findings, and how promptly results must be shared with the state.

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency	SIPM	

The purpose of this question is to validate that the vendor will be able to prove that appropriate controls are in place and operating effectively in order to protect the state's data and investment. See the guide for Section 1, Question 5 for more background information.

APPROVING BUSINESS OWNER SIGNATURE

First name Last name Title Click here to enter a date

X

APPROVING TECHNOLOGY MANAGER SIGNATURE

First name Last name Title Click here to enter a date

X

ESO SIGNATURE

First name Last name Title Click here to enter a date

X

See the guide in Section A for information about who should sign. When so required, the agency must submit this section for OSCIO approval before proceeding.

GUIDANCE ON SECTION C: (RENEWAL/REUSE)

Required only for renewals of previously-approved solutions

Purpose of this form: To identify whether any substantive requirements have changed since last approval of a cloud and hosted system.

Is the agency required to complete this form? The agency must complete this section only when seeking to renew (extend or amend) a contract for a cloud and hosted system investment that was previously approved by OSCIO.

What if there was no past approval? If the investment meets thresholds for requiring OSCIO approval but has never received approval, then the agency must use the regular cloud & hosted systems procedure.

When must the agency complete this form? This section must be completed before the agency amends a contract or renews a service.

Is OSCIO approval required? If here have been substantive changes to any requirements since the investment was approved by OSCIO, then OSCIO approval for this section must be obtained before executing a contract, purchase order, or other binding document. Submit together with the previously approved workbook.

Agency/division: Enter agency name and division

IT Service/Product name: Enter service or product name

Agency contact name, email address, and phone number:

First name Last name
Email address Phone number

ESO contact name, email address, and phone number:

First name Last name

Email address Phone number

The IT service/product name should match that previously used.

C1: Have any elements addressed in the Risk Factor Determination section of this Workbook (also known as Section A of the Workbook) changed in such a way that the risk has changed from Low to Significant?

☐ No, risk has not changed.

☐ Yes, risk has changed from Low to Significant. **-> If checked, update impacted answers in Section A & B of the workbook and submit to OSCIO for approval.**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency	SIPM	

C2: Have Agency security, incident response, or other nonfunctional requirements addressed in Section 2 changed substantively since the last approval?

☐ No, agency requirements have not changed substantively.

☐ Yes, agency requirements have changed substantively. **-> If checked, update impacted answers in Section B of the workbook and submit to OSCIO for approval.**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

C3: Have State or other applicable security, incident response, or other policies or requirements addressed in Section 2 changed substantively since the last approval?

☐ No, neither state nor other applicable requirements have changed substantively.

☐ Yes, state and/or other applicable requirements have changed substantively. **-> If checked, update impacted answers in Section B of the workbook and submit to OSCIO for approval.**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency & ESO	Agency		

C4: Are there any OSCIO-supplied conditions related to this Service for which OSCIO has not acknowledged agency compliance? Such conditions are typically included in an approval memo.

☐ No, there are no outstanding conditions; OSCIO has acknowledged compliance with any related conditions.

☐ Yes, there are outstanding conditions. **-> If checked, seek approval from OSCIO before continuing.**

Responsibility Assignment Matrix	Responsible	Accountable	Consulted	Informed
	Agency EITG	Agency	ESO	

DOCUMENT REVISION HISTORY

This document contains the *Document Revision History* for both the Guide and Workbook:

Workbook Revision History

Version	Date	Description
1.0		Creation
2.0	4/25/2019	Major update: Created short and long versions based on risk category

Guide Revision History

Version	Date	Description
1.0	n/a	Skipped to align with V2.0 of Cloud Policy and Workbook updates
2.0	4/25/2019	Creation; aligned with workbook version 2 to align with changes