

DEPARTMENT OF FINANCE

**Information Technology  
Project Oversight  
Framework**



**This Page Intentionally Left Blank**

# Table of Contents

<b>SECTION 1: INTRODUCTION AND OVERVIEW .....</b>	<b>1</b>
<b>SECTION 2: PROJECT CLASSIFICATION FOR OVERSIGHT .....</b>	<b>7</b>
<b>SECTION 3: DEPARTMENT PROJECT MANAGEMENT REQUIREMENTS .....</b>	<b>11</b>
<b>SECTION 4: FINANCE PROJECT MANAGEMENT PRACTICES ASSESSMENT .....</b>	<b>17</b>
<b>SECTION 5: RISK MANAGEMENT AND ESCALATION PROCEDURES .....</b>	<b>21</b>
<b>SECTION 6: INDEPENDENT OVERSIGHT REQUIREMENTS .....</b>	<b>25</b>
<b>APPENDIX A: REQUIRED PROJECT MANAGEMENT PRACTICES AND PRODUCTS .....</b>	<b>29</b>
<b>APPENDIX B: DEPARTMENT PROJECT MANAGEMENT ASSESSMENT FORM .....</b>	<b>35</b>
<b>APPENDIX C: CATEGORIES AND EXAMPLES OF RISK.....</b>	<b>43</b>
<b>APPENDIX D: PROJECT RISK LIST.....</b>	<b>49</b>
<b>APPENDIX E: RISK MANAGEMENT FORM.....</b>	<b>51</b>
<b>APPENDIX F: PROJECT OVERSIGHT REVIEW CHECKLIST .....</b>	<b>53</b>
<b>APPENDIX G: INDEPENDENT PROJECT OVERSIGHT REPORT.....</b>	<b>63</b>
<b>APPENDIX H: DEFINITION OF TERMS .....</b>	<b>75</b>

**This Page Intentionally Left Blank**

## Section 1: Introduction and Overview

Executive Order D-59-02 and Management Memo 02-16 assigned responsibilities for information technology (IT) management and oversight following the sunset of the Department of Information Technology on June 30, 2002. Those documents outline an approach that vests IT management responsibilities with each department director, and oversight responsibilities with each Agency. For departments operating outside Agencies, the department director is vested with both management and oversight responsibilities.

The Budget Act of 2002 created IT oversight and security programs within the Department of Finance (Finance). Budget Letter (BL) 02-37 described Finance's oversight program objectives and the roles and responsibilities of departments, Agencies and Finance regarding statewide IT oversight. Finance's overriding objectives for oversight are:

- Implement an effective system of independent graduated oversight for all IT projects
- Establish statewide standards for project management and oversight
- Assess current department/Agency IT project management and oversight practices

BL 02-37 also described Finance's immediate objective to create a framework for effective oversight of IT projects. This document provides the oversight framework outlined in BL 02-37.

### Key Concepts

The framework described in this document is based upon several key concepts set forth in BL 02-37, and applies to all reportable IT projects as defined in the State Administrative Manual (SAM), Section 4800.

### Definition of Project Oversight

BL 02-37 defines project oversight as “an *independent* review and analysis... to determine if the project is on track to be completed within the estimated schedule and cost, and will provide the functionality required by the sponsoring business entity. Project oversight identifies and quantifies any issues and risks affecting these project components.” The framework described in this document emphasizes the independent nature of project oversight, along with the requirements for risk identification and mitigation.

## Graduated Oversight

Departments must implement independent oversight for all reportable projects. Critical projects must receive additional oversight from the appropriate Agency (or Finance, for departments operating outside Agencies) and the most critical projects will receive additional oversight from Finance. This document describes the criteria Finance will use to identify the level of criticality and oversight for IT projects.

## Project Management Practices and Processes

Finance will assess department/Agency project management practices and processes as demonstrated on current projects. The framework described in this document outlines the *minimum* practices and processes that must be in effect to support successful IT projects. These practices and processes will form the basis for Finance to perform their assessments.

## Components of the Framework

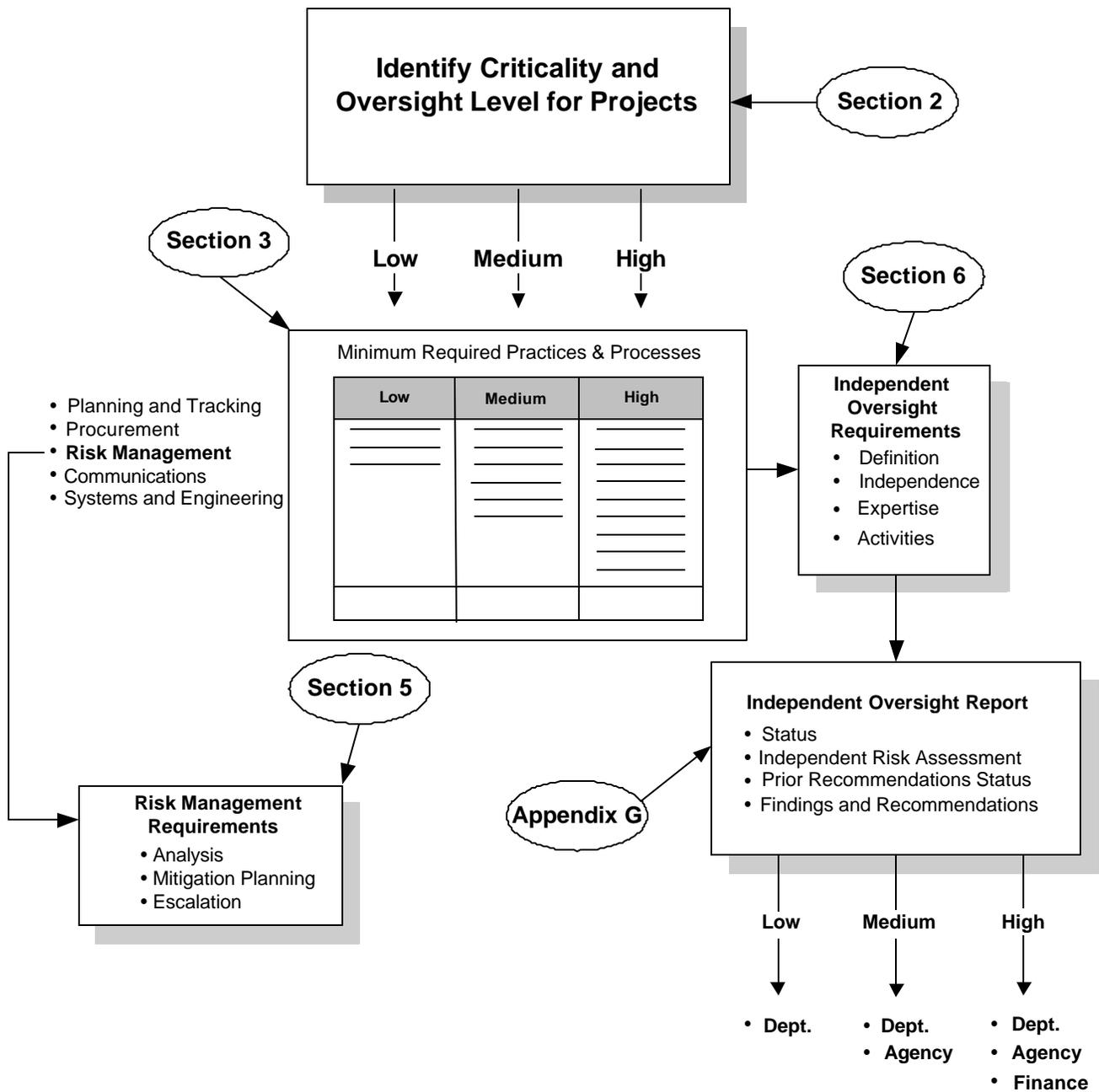
The framework for graduated project oversight will be used to assess the risk, sensitivity and/or criticality of IT projects. This assessment will place each individual project into one of three categories (low, medium, or high). All projects will receive department level oversight, critical (medium) projects will receive additional oversight from the appropriate Agency (or Finance for departments operating outside Agencies) and the most critical (high) projects will receive additional oversight from Finance. Finance has completed an initial assessment of projects currently in progress and has identified the oversight category for each project. The criteria for project assessment are covered in **Section 2** of this document.

Finance will establish statewide standards for project management and oversight, and initial criteria for assessing department/Agency project management and oversight practices. Finance will also evaluate the demonstrated degree to which the departments/Agencies have established project management and internal project oversight practices and processes. **Section 3** of this document describes a *minimum required* set of practices and products that will form the basis for assessing and evaluating department/Agency performance in both project management and project oversight. The required set of practices and products is tailored to the three categories of project criticality. **Section 4** defines the IT structure and environment components used to assess department/Agency project management practices.

Finance has placed a significant emphasis on risk management as a critical function within the oversight framework. The framework directs that project oversight entities identify and quantify any issues and risks, and that appropriate notification of project risks to the Agency level (from departments) and to Finance (from Agencies) is an essential part of effective oversight. Furthermore, project managers are expected to establish appropriate remediation plans for the identified project risks. **Section 5** of this document contains the *minimum* requirements for risk management, to be implemented on *all* IT projects.

As noted above, Finance will establish statewide standards for project management and *oversight*, and initial criteria for assessing department/Agency project management and *oversight* practices. Finance will evaluate the demonstrated degree to which the departments/Agencies have established project management and internal project *oversight* practices and processes. **Section 6** of this document contains the *minimum* requirements for project oversight, to be implemented on *all* IT projects. The oversight requirements emphasize risk identification and reporting, along with the need for independent review of the performance of the activities required by the *minimum* set of practices and products described in Section 3.

## Project Oversight Framework Components



## Implementation of the Framework

The flow diagrams on the following two pages illustrate the major entities and flows of information involved in implementing the oversight framework described in this document. Figure 1.2 highlights the roles of departments, Agencies and independent oversight, showing the flow of oversight reporting and risk escalation. Figure 1.3 highlights the role of Finance in administering the oversight framework, assessing department/Agency capabilities and individual project criticality, and providing additional oversight to the State's most critical IT projects.

## Forms and Templates

BL 02-37 states that Finance will establish "initial project oversight reporting forms."

The appendices to this report contain the templates briefly described below. The Section of this document where each template is referenced is shown in parenthesis.

Appendix A – Project Management Practices and Processes (Sections 3 and 6). Contains the specific practices and processes that are required, based on the project criticality level, for all IT projects.

Appendix B – Project Management Capability Assessment Checklists (Section 3). Transforms the practices and processes described in Appendix A into questionnaire/checklist format for use by Finance in assessing department/Agency project management practices.

Appendix C – Categories and Examples of IT Project Risk (Section 5). Provides information useful to departments and Agencies in the project risk identification process.

Appendix D – Project Risk List (Section 5). Provides a template for departments for recording project risks and their attributes.

Appendix E – Risk Management Form (Section 5). Provides a template for departments for tracking individual risk information within an ongoing project risk management program and the means for escalating project risks as described in Section 5.

Appendix F – Project Oversight Checklists (Section 6). Transforms the practices and processes described in Appendix A into questionnaire/checklist format for use in independent oversight reviews of individual projects.

Appendix G – Project Oversight Report (Section 6). Provides a template for the written project oversight report format to be submitted by independent oversight providers to departments, Agencies and Finance under the graduated oversight approach.

Appendix H – Definition of Terms.

Figure 1.2 – Department/Agency/Independent Oversight

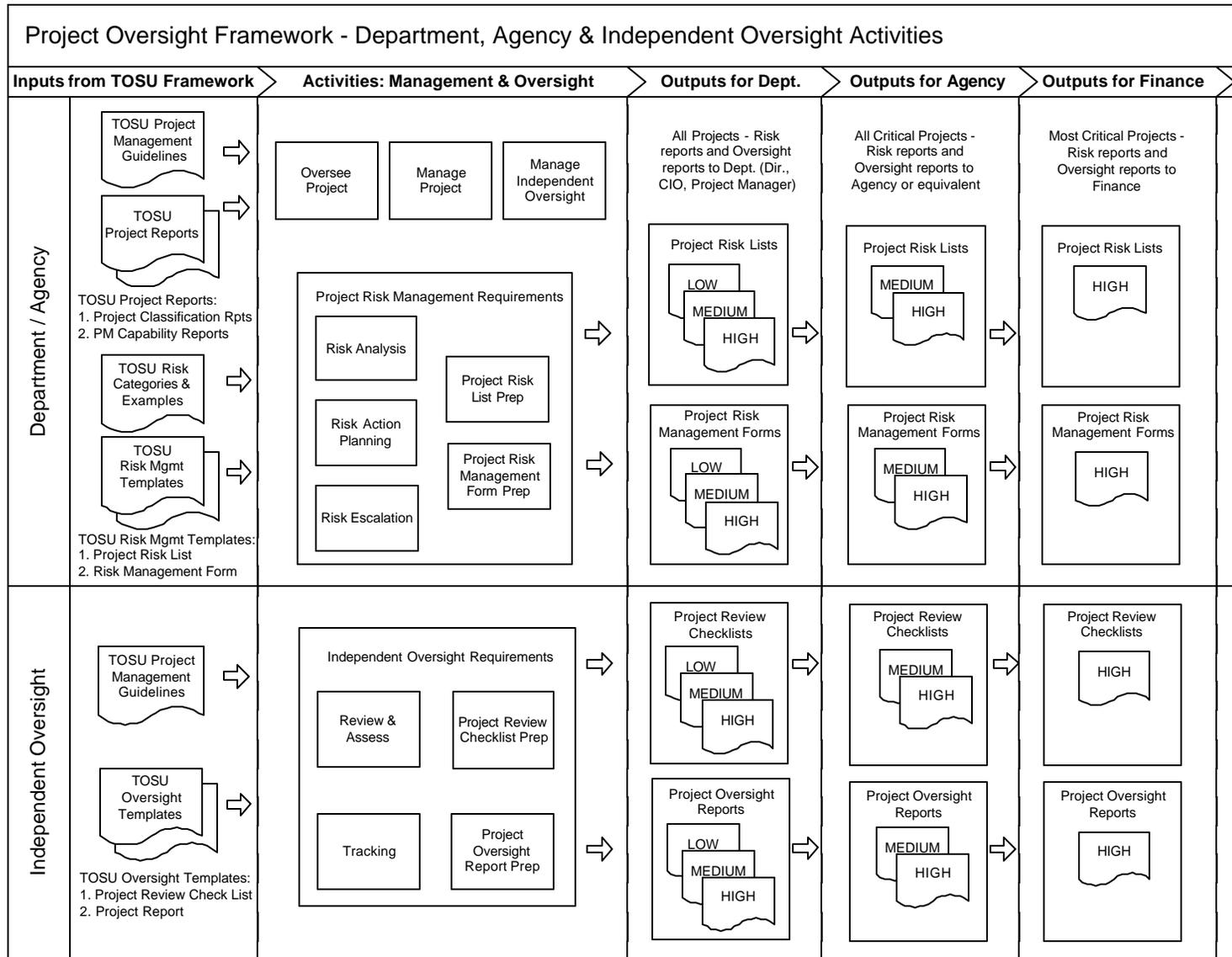
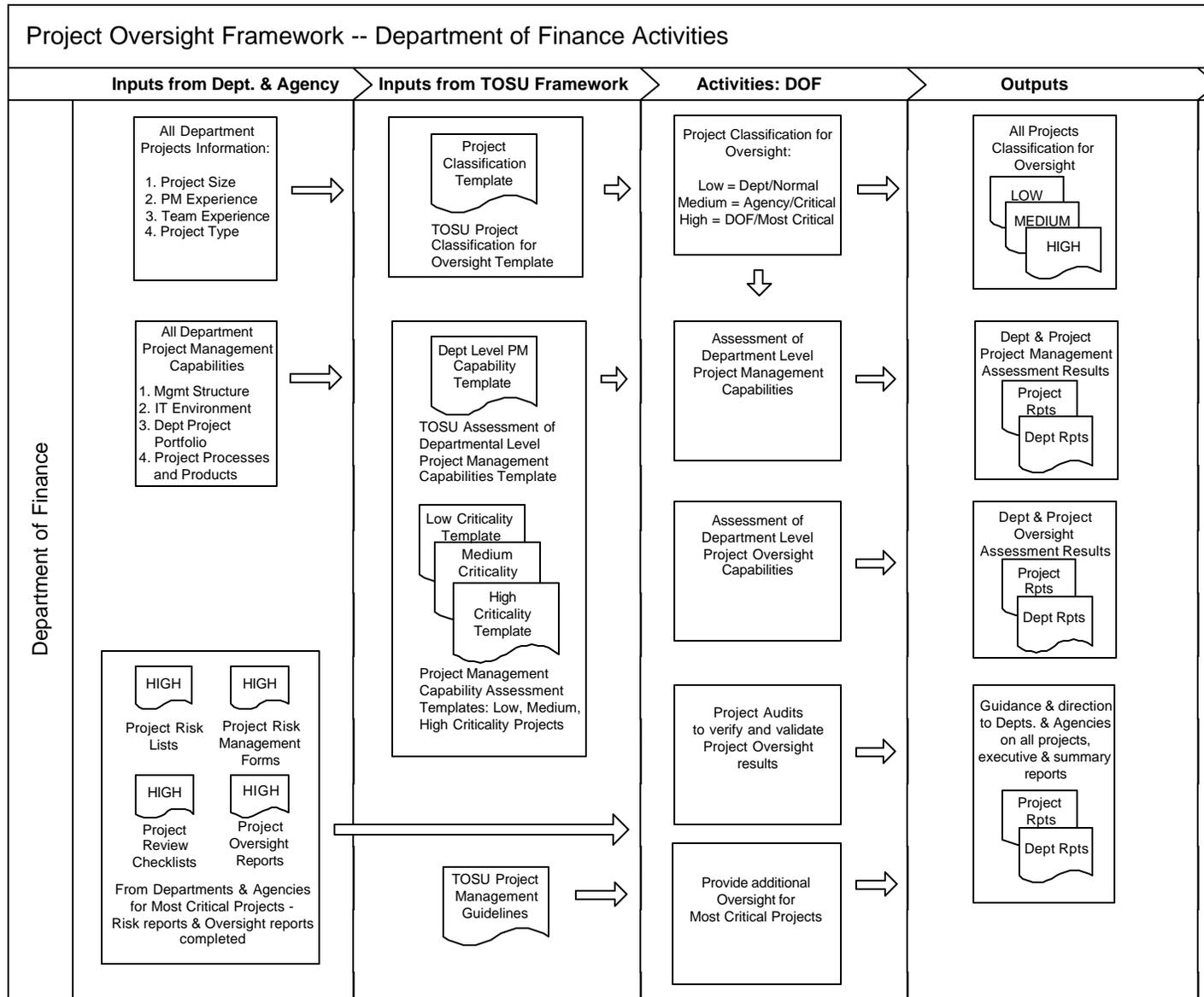


Figure 1.3 – Role of Finance



Section  
2

## Section 2: Project Classification for Oversight

This section describes the process Finance will use to establish criticality/risk and oversight level of IT projects. The process is designed to assess the risk, sensitivity and/or criticality of IT projects and does so by assigning ratings of low, medium and high to four project specific factors and assigning the average of the four factors to the project. The four project specific factors are project size, project manager experience, team experience and project type. Finally, an assessment of external factors affecting the project, or past project performance within the department, may result in an adjustment to the risk/criticality rating. The steps for determining a project’s classification are described below.

### Determine The Risk/Criticality Rating For Each Project Evaluation Factor

#### Factor 1: Project Size

This factor rates the project on size, primarily based upon one time cost estimates and secondarily, upon project duration.

Step 1: Rate the project by estimated one-time costs at follows:

Estimated one-time Costs	Rating
Greater than \$10 million	High
\$5 million to \$10 million	Medium
Under \$5 million	Low

Step 2: Adjust low and medium ratings from Step 1 upward by one rating if the estimated period from project approval to initial implementation is greater than 24 months.

#### Factor 2: Project Manager Experience

This factor rates the risk/criticality based on the project manager’s experience on similar efforts.

Project Manager	Rating
Has not completed a like project in a "key staff" role	High

Project Manager	Rating
Has completed one like project in a "key staff" role	Medium
Has completed two or more like projects in a "key staff" role	Low

Please refer to Appendix H - Definitions of Terms for further explanations of the terms *key staff*, *like project*, and *completed*.

Factor 3: Team Experience

This factor rates the risk/criticality based on the experience of the project team key staff. The project team consists of all project staff reporting to the state project manager, including contractor staff, if applicable.

Step 1: Evaluate the experience of each key staff member, including contractor staff, for completion of like projects in key roles.

Step 2: Determine what proportion of the key staff members have completed similar projects in key roles. Assign the team experience rating as follows:

Like Projects Completed by at Least 75% of Key Staff	Rating
None	High
One	Medium
Two or more	Low

Factor 4: Project Type

This factor rates the technical complexity of the work being undertaken.

Step 1: Using Table 2.1 on the following page, "Elements of Project Type," circle the rating for each applicable element. Refer to Appendix H - "Definition of Terms" for explanations of each element.

Step 2: Assign the rating for this factor based upon the highest rating from among all of the elements circled in Step 1.

Table 2.1: Elements of Project Type

Component	Activity Category	Affected Element	Rating
Hardware	New Install	Local Desktop / Server	Low
		Distributed / Enterprise Server	Medium
	Update / Upgrade	Local Desktop / Server	Low
		Distributed /Enterprise Server	Low

Component	Activity Category	Affected Element	Rating
	Infrastructure	Local Network / Cabling	Low
		Distributed Network	Medium
		Data center / Network Operations Center	High
Software	Custom Development	Local Desktop / Server	Low
		Distributed / Enterprise Server	High
	COTS Installation (new)	Local Desktop / Server	Low
		Distributed / Enterprise Server	High
	Custom Update / Upgrade	Local Desktop / Server	Low
		Distributed / Enterprise Server	High
	COTS Update / Upgrade	Local Desktop / Server	Low
		Distributed / Enterprise Server	Medium
	Infrastructure	Middleware	Medium
		Layered Product	Medium
		DBMS	Medium

Computation of the Overall Project rating

After determining the rating for each evaluation factor, a single rating of high, medium, or low must be assigned to each project.

Step 1: Enter the individual factor rankings in column (b), lines 1 through 4, in Table 2.2 below and determine the total for column (b). Use 3 for high, 2 for medium, and 1 for low.

Table 2.2 Compute Project Score

	(a) Factor	(b) Rating
1	Size	
2	Project Manager	
3	Project Team	
4	Type	
	Total	

Step 2: Compute the project score by dividing the total from column (b) by four.

Step 3: Assign the overall project ranking by selecting high, medium, or low from Table 2.3 below, using the value determined in Step 2 above.

Table 2.3: Assignment of Project Rating

<b>Results</b>	<b>Project Rating</b>
2.26 – 3.0	High
1.51 – 2.25	Medium
1.0 – 1.5	Low

Finance may raise the rating of project oversight based on additional factors such as past project performance by the sponsoring department or substantial risks identified with the project.

## Section 3: Department Project Management Requirements

This section presents the *minimum required* practices and processes for reportable (SAM Section 4800) IT projects. These requirements are consistent with industry standards and accepted best practices such as the Project Management Institute’s “Project Management Body of Knowledge” and the Institute of Electrical and Electronics Engineers, Inc. standards. Finance does not require departments to adopt any specific industry standard or set of standards for project management or system development. The practices and processes described below will form the principal basis for Finance’s assessment to determine the effectiveness of department/Agency IT project management activities.

### Minimum Requirements for Project Management Practices and Processes

Required minimum project management practices and processes have been defined for each level of project criticality, as described in Section 2. These requirements represent a synthesis of the most basic best practices in IT project management. They are presented under five categories:

1. Planning and Tracking
2. Procurement
3. Risk Management
4. Communications
5. System Engineering

Their descriptions are specifically intended to leave the details of implementation subject to the discretion of the departments. They are presented in Appendix A and on the Tables shown in the following pages. It is expected that many departments have established project management practices beyond those included in the framework. Finance’s assessments of department project management capabilities will be based on the requirements included in the framework. However, Finance will recognize departments that perform beyond the minimum required level.

Table 3.1: Required project management practices and processes for Low criticality projects

	<b>Low</b>
<b>Planning and Tracking</b>	Formal identification of the project business case, project goals, objectives, expected outcomes, key stakeholders, sponsor(s), etc. (i.e. project charter)
	Development and maintenance of a project work plan including identification of activities, milestones and schedule
	Development and maintenance of a project organization chart
	Development and maintenance of project cost estimates and supporting data for each cost category
	Recording of actual costs by cost category and comparing actual costs to budget
	Maintenance of supporting data for actual costs
	Tracking and reporting (within status reporting process) of work plan activities, schedule and milestone completion status
	Change control/approval for key specification documents (e.g. contracts, requirement specifications and other contract deliverables) and software products
	Tracking of issues/problems and their resolution
	Assessment of user satisfaction at key milestones
	Project closeout activities, including a PIER, collecting and archiving up-to-date project records and identifying lessons learned
<b>Procurement</b>	Use of appropriate procurement vehicle
	Inclusion of a detailed written scope of work for services requested in solicitation document
<b>Risk Management</b>	Identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines
<b>Communications</b>	Regular status reporting to key stakeholders, including progress against timeline and budget; risk management results and status; issue management results and status
<b>System Engineering</b>	Formal user approval/sign-off on written specifications
	Formal testing and user sign-off of test results and completed system

Table 3.1: Required project management practices and processes for Medium criticality projects

	<b>Medium</b>
<b>Planning and Tracking</b>	Formal identification of the project business case, project goals, objectives, expected outcomes, key stakeholders, sponsor(s), etc. (I.e. project charter)
	Detailed project planning with all activities (tasks), milestones, dates and estimated hours by task loaded to project management software; lowest level tasks of short duration with measurable outcomes
	Completion of planned tasks recorded within PM software
	Actual hours expended by task recorded at least monthly within PM software
	Estimated hours to complete by task recorded at least monthly within PM software
	Development and maintenance of a project organization chart
	Development and maintenance of project cost estimates and supporting data for each cost category
	Use of formal software size estimation where custom software development or COTS modifications are a significant component of cost
	Use of two or more estimation approaches (e.g. top-down, bottom-up, parametric) to refine estimates
	Recording of actual costs by cost category and comparing actual costs to budget
	Maintenance of supporting data for actual costs
	Tracking and reporting (within status reporting process) of work plan activities, schedule and milestone completion status
	Change control/approval for key specification documents (e.g. contracts, requirement specifications and/or contract deliverables) and software products
	Formal tracking of issues/problems and their resolution, including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities
	Assessment of user satisfaction at key milestones
Completion of project closeout activities, including a PIER, collecting and archiving up-to-date project records and identifying lessons learned	
<b>Procurement</b>	Use of appropriate procurement vehicle
	Inclusion of a detailed written scope of work for services requested in solicitation document
	Detailed requirements specifications included in solicitation document
<b>Risk Management</b>	Identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines
<b>Communications</b>	Formal communications management, including a written project communications plan. Regular status reporting to key stakeholders, including progress against timeline and budget; risk management results and status; issue management results and status; Written escalation policy for issues and risks; Regular stakeholder involvement in major project decisions, issue resolution and risk mitigation
<b>System Engineering</b>	Ongoing user involvement commensurate with user impact
	Formal user approval/sign-off on written specifications
	Adherence to a formal system development life-cycle (SDLC) methodology
	Tracking requirements traceability through all life-cycle phases
	Adherence to software engineering standards
	Software defect tracking beginning with unit testing
	Performance of formal code reviews
	Formal quality assurance through all life-cycle phases
Formal testing and user sign-off of test results and completed system	

Table 3.1: Required project management practices and processes for High criticality projects

	<b>High</b>
<b>Planning and Tracking</b>	Formal identification of the project business case, project goals, objectives, expected outcomes, key stakeholders, sponsor(s), etc. (I.e. project charter)
	Detailed project planning with all activities (tasks), milestones, dates and estimated hours by task loaded to project management software; lowest level tasks of short duration with measurable outcomes
	Completion of planned tasks recorded within PM software
	Actual hours expended by task recorded at least monthly within PM software
	Estimated hours to complete by task recorded at least monthly within PM software
	Formal staff planning, including organization chart, written roles and responsibilities, plans for staff acquisition, schedule for arrival and departure of specific staff, and staff training plans
	Development and maintenance of project cost estimates and supporting data for each cost category
	Use of formal software size estimation where custom software development or COTS modifications are a significant component of cost
	Use of two or more estimation approaches (e.g. top-down, bottom-up, parametric) to refine estimates
	Independent review of estimates
	Recording of actual costs by cost category and comparison to budget
	Maintenance of supporting data for actual costs
	Tracking and reporting (within status reporting process) of work plan activities, resource utilization, schedule and milestone completion status
	Formal configuration control, including a written configuration management plan covering change control/approval for key specification documents (e.g. contracts, requirement specifications and/or contract deliverables) and software products and specific staff roles and responsibilities for configuration management
	Formal tracking of issues/problems and their resolution, including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities
	Assessment of user satisfaction at key milestones
	Planning in compliance with formal standards or system development life-cycle (SDLC) methodology
Formal enterprise architecture planning	
Completion of project closeout activities, including a PIER, collecting and archiving up-to-date project records and identifying lessons learned	
<b>Procurement</b>	Use of appropriate procurement vehicle
	Inclusion of a detailed written scope of work for services requested in solicitation document
	Detailed requirements specifications included in solicitation document
	Material participation of outside expertise (e.g. DGS, Departmental specialists, consultants)
	Consultation with qualified legal counsel for procurement if outsourcing
<b>Risk Management</b>	Formal continuous risk management, including development of a written risk management plan, identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines, and regular management team review of risks and mitigation progress
	Use of SEI "Taxonomy Based Questionnaire" or similar risk identification aid(s)
<b>Communications</b>	Formal communications management, including a written project communications plan. Regular status reporting to key stakeholders, including progress against timeline and budget; risk management results and status; issue management results and status; Written escalation policy for issues and risks; Regular stakeholder involvement in major project decisions, issue resolution and risk mitigation

High	
<b>System Engineering</b>	Ongoing user involvement commensurate with user impact
	Formal user approval/sign-off on written specifications
	Adherence to a formal system development life-cycle (SDLC) methodology
	Use of requirements management software and tracking of requirements traceability through all life-cycle phases
	Adherence to software engineering standards
	Product defect tracking beginning with Requirements Specifications
	Performance of formal code reviews
	Formal quality assurance through all life-cycle phases
	Formal testing and user sign-off of test results and completed system
	Adherence to an enterprise architecture plan
	Deliverable inspections, beginning with requirements specifications
	Formal IV&V

**This Page Intentionally Left Blank**

Section  
**4**

## Section 4: Finance Project Management Practices Assessment

The following pages present the steps Finance will follow when rating departmental project management capabilities as high, medium, or low. The components of the assessment are based upon two factors, 1) the department’s IT management structure and environment and 2) the degree to which the required framework components are effectively used on department IT projects.

### IT Management Structure and Environment Assessment Criteria

Finance will assess the following six components for each department:

<b>Executive level visibility and control of the IT function</b>	
The Department has a position responsible for all Department IT projects (e.g. CIO) that reports to the Director or a Deputy Director.	High
The individual responsible for all Department IT projects has either (1) responsibility for non-IT as well as IT functions or (2) does not report to the Director or a Deputy Director.	Medium
There is no single individual responsible for all Department IT projects.	Low

<b>Centralization of PM support and related functions</b>	
The Department has a unit that is independent of any individual project that provides project management office (PMO) type support for all department projects and project managers.	High
The Department has specialists in IT planning, budgeting, tracking and control agency reporting, but does not possess an IT PMO-type organization; or the department’s PMO-type organization does not support all department projects.	Medium
The Department possesses neither of the above.	Low

<b>Training and Certification of Project Managers</b>	
The Department formally supports/ sponsors formal training for IT project managers and staff participate in training and, as appropriate, have become formally certified.	High
While there is no formal Department support/sponsorship for formal training for IT project managers, Department staff participate in formal training and, as appropriate, have become formally certified.	Medium
Department staff do not participate in formal project management training/certification programs.	Low

<b>Use of a Formal Project Management Methodology</b>	
The Department uses (and/or requires contractors to use) a single formal methodology for project management functions on all projects.	High
The Department (and/or requires contractors to use) adheres to specific formal standards for project management functions on projects or uses multiple formal methodologies.	Medium
The Department does not always use, nor does it require contractors to always use, a formal project management methodology.	Low

<b>Use of a Formal System Development Methodology</b>	
The Department uses (and/or requires contractors to use) a single formal system development life cycle methodology on all IT projects.	High
The Department uses (and/or requires contractors to use) multiple formal system development methodologies with each project adhering to one.	Medium
The Department does not always use, nor does it require contractors to always use, a formal system development life cycle methodology.	Low

<b>Enterprise Architecture Strategy</b>	
The Department has a comprehensive enterprise hardware/software architecture strategy and uses the strategy to guide project level architecture decisions.	High
The Department lacks a comprehensive enterprise architecture strategy, but technical architecture standards and guidelines are generally understood and followed on individual projects.	Medium
The Department lacks any enterprise architecture strategy, or generally does not follow any enterprise hardware/software standards.	Low

Computation of the IT Management Structure and Environment Rating

Step 1: Enter the individual factor rankings in column (b), lines 1 through 6, in Table 4.1 below and determine the total for column (b). Use 3 for high, 2 for medium, and 1 for low.

Table 4.1: Compute IT Management Structure and Environment Score

<b>(a) Factor</b>		<b>(b) Rating</b>
1	Executive Level Visibility and Control	
2	Centralization of PM Support	
3	Training and Certification of Project Managers	
4	Project Management Methodology	
5	System Management Methodology	
6	Enterprise Architecture Strategy	
Total		

Step 2: Compute the score by dividing the total from column (b) by six.

Step 3: Assign the IT Management Structure and Environment ranking by selecting high, medium, or low from Table 4.2 below, using the value determined in Step 2 above.

Table 4.2: Assign IT Management Structure and Environment Rating

<b>Possible Results</b>	<b>Recommended Project Rating</b>
2.51 – 3.0	High
1.71 – 2.5	Medium
1.0 – 1.7	Low

Project Management Practices and Processes Assessment

Finance will assess the degree to which departments have established and used the required project management practices documented in this framework. Finance will review multiple projects, at multiple levels of criticality for departments to establish an overall project management capability for the department. Finance will interview the appropriate department IT management and staff, review project documents, and observe the project team and project activities to determine the degree to which the requirements are being met. A sample project management assessment form, based on the framework requirements, is included as Appendix B. The form will be used to determine if the required project management activities have been effectively performed on all, some or none of the projects reviewed.

Complete the summary Project Management Assessment Form, Appendix B. Assign points to each answer, three points for *All*, one point for *Some* and zero points for *None*.

After completing the applicable questionnaires, based on project criticality level, compute the total number of points for each and assign a ranking for each type of project in accordance with Table 4.3. A department may have up to three assigned rankings; one for each level of project criticality.

Table 4.3: Project Practices and Processes Assessment Rating

Questionnaire Completed	Assign a ranking of High for	Assign a ranking of Medium for	Assign a ranking of Low for
High criticality projects	Greater than 121	88-121	Less than 88
Medium criticality projects	Greater than 91	66-91	Less than 66
Low criticality projects	Greater than 53	39-53	Less than 39

Assignment of Overall Department Rating

The overall assessment rating for a department is expressed in terms of the two components: (1) IT management structure and environment and (2) implementation of the required project management practices and processes. Therefore, a department will have between two and four ratings, a single rating for IT management structure and environment and one rating for each type (level of criticality) of project that it performs.

A gray rectangular box containing the word "Section" in a black serif font at the top, and a large white number "5" in a sans-serif font below it.

## Section 5: Risk Management and Escalation Procedures

This Section presents the minimum risk management requirements for all reportable IT projects. The project risk management requirements include the following three major components:

- Risk Analysis. This component covers the six steps necessary to identify, analyze and prioritize risks.
- Risk Action Planning and Tracking. This component includes a template for risk planning and tracking covering the most critical components of ongoing risk management.
- Risk Escalation. This section presents escalation criteria based upon project criticality and risk severity.

All projects should formally review risks at least monthly. Risks should be reviewed by a group of individuals representing all components of the project organization, to ensure identification of all risks.

### Risk Analysis

Basic risk analysis consists of three activities: identification of risks, assignment of risk attributes, and determination of risk severity. These activities are further described below, followed by a six-step approach to their implementation.

#### Identify Risks

Project risks should be identified in terms of specific concerns, problems or possible future occurrences that could result in negative impacts on project budget, schedule, or quality. Quality is broadly defined to include such important objectives as functionality, performance, usability and other similar functional, technical and performance objectives. Step 1, below describes how to identify and record project risks.

#### Assign Risk Attributes: Impact, Likelihood and Time Frame

Basic risk analysis involves understanding the impact of the negative consequence identified for each risk, and the probability, or likelihood, of occurrence of that consequence. In addition, a time frame is assigned to each risk, representing how soon action is required to prevent the risk from occurring. While necessarily subjective, assignment of these attributes should be based upon the best information and analysis available to the project manager. Steps 2, 3 and 4, below, describe how to assign the three key risk attributes.

## Determine Risk Exposure and Risk Severity

It is essential to rank or prioritize risks to understand the greatest potential threats to the project and to effectively plan and perform mitigation efforts. Using the ratings for impact, probability and time frame, risk severity is determined as described in Steps 5 and 6 below.

### Step 1: Identify Project Risks

Use Appendix C: **Categories and Examples of Risks**, or a similar aid, to assist in identifying specific risks that are present on a particular project in each of the eleven checklist categories. The attachment presents representative concerns or problems that are often sources of risk on IT projects. It is meant to be an *aid in risk identification*, not a comprehensive and complete list of possible risks.

A risk statement is a concise declaration of risk using a standard notation or sentence structure:

*Concern • Likelihood • Consequence*

Examples of typical risk statements include:

Mandated unrealistic implementation date • will almost certainly • lead to significant missing functionality in the implemented system.

Late contractor deliverables • will likely • result in delayed pilot testing.

Regulation changes • may • result in the need for costly change orders and/or delayed implementation.

List brief statements describing each identified risk on Appendix D, **Project Risk List**

Step 2: Assign an Impact rating of High, Medium, or Low to each identified risk.

For impact, if the risk represents a significant negative impact on project budget, schedule, or quality, it should be rated high. Material impacts would significantly affect users, clients, or other key stakeholders, and should be rated medium. If the risk does not represent a significant or material impact on project budget, schedule or quality, it should be rated low. Record the expected impact for each risk on the **Project Risk List**.

Step 3: Assign a probability rating of High, Medium, or Low to each identified risk.

For probability, risks considered as almost certain or very likely to occur should be rated high. Risks that may occur or have a 50/50 chance of occurring should be rated medium. Risks considered unlikely to occur or that will probably not occur should be rated low. Record the expected probability for each risk on the **Project Risk List**.

Step 4: Assign a time frame for mitigation to each identified risk.

Next, the time frame within which action must be taken in order to successfully mitigate the risk should be rated. If the time frame is less than six months, assign a rating of Short; for 6 months to one year assign a rating of Medium; and for greater than one year, assign a rating of Long.

Record the time frame for each risk on the **Project Risk List**.

Step 5: Determine Risk Exposure

Risk exposure is derived from the risk attributes impact and probability, and is used, in conjunction with time frame, to prioritize risks for mitigation and escalation. Determine risk exposure for each risk from the intersection of that risk’s impact and probability in the matrix below.

Risk Exposure Matrix

		Probability		
		High	Medium	Low
Impact	High	<b>High</b>	<b>High</b>	Medium
	Medium	<b>High</b>	Medium	Low
	Low	Medium	Low	Low

Record the exposure for each risk on the **Project Risk List**.

Step 6: Determine Risk Severity

Risk severity is a function of exposure (from Step 5 above) and time frame and determines the relative priority of the identified risks. Determine risk severity for each risk from the intersection of that risk’s exposure and time frame in the matrix below.

Risk Severity Matrix

		Exposure		
		High	Medium	Low
Time Frame	Short	<b>High</b>	<b>High</b>	Medium
	Medium	<b>High</b>	Medium	Low
	Long	Medium	Low	Low

Record the severity for each risk on the **Project Risk List**.

Risk Action Planning

The project must develop an action plan for each identified risk and track progress against the plan.

If the project can continue and be successful with the anticipated impact of the risk, the project may choose to *accept* the risk, document the acceptance, and expend no further resources managing it.

If the risk cannot be accepted and there is action that can or must be taken, then *mitigate* the risk by developing and implementing a mitigation plan. Often, a simple list of action items, with responsibilities and due dates identified, will be an adequate plan. For projects of high and medium criticality, some high severity risks may require more elaborate mitigation planning. For example, a formal work breakdown structure (WBS) and resource budget may be required for particularly complex or high impact risks.

The minimum elements required for a risk planning and tracking process are shown in the **Risk Management Form** (Appendix E.) A risk management form must be completed for all Medium and High project risks. These risks must be reviewed and tracked monthly.

Risk Escalation

Depending upon risk severity, as determined in Step 6 above, and project criticality, some risks will be escalated from department to Agency, and from Agency to Finance. Not all risks require escalation and escalation of project risks will *not* necessarily result in a change in project criticality.

Risk escalation requirements are shown in the risk escalation matrix, below. Departments or Agencies must provide a current **Risk Management Form** to the Agency or Finance, respectively, within 15 calendar days of determination that the escalation requirements have been met.

Risk Escalation Matrix

		Risk Severity		
		High	Medium	Low
Project Criticality	High	To Finance	To Agency	Department (No escalation)
	Medium	To Agency		Department (No escalation)
	Low	To Agency	Department (No escalation)	



## Section 6: Independent Oversight Requirements

This Section presents the minimum requirements for independent oversight of all reportable projects. Each department is responsible for providing independent oversight of all reportable projects within the department. Agencies must provide additional oversight for all projects within the agency that are assigned a medium or high level of criticality/risk. Finance will provide additional oversight for all projects assigned a high level of criticality/risk.

### Definition of Project Oversight

Project oversight is an independent review and analysis of specific project activities and documentation to determine if the project is on track to be completed within the estimated schedule and cost, and will provide the functionality required by the sponsoring business entity. Project oversight identifies and quantifies any issues and risks affecting these project components.

### Essential Attributes of an Oversight Team

An oversight team must possess two essential attributes: independence and expertise.

#### Independence

The approach to meeting the independence requirement varies by project criticality. For high criticality projects, the oversight must be conducted by consultants (contractors) engaged by the department. Oversight consultants will provide formal oversight reports concurrently to both the Agency and Finance. For low and medium criticality projects, the oversight team *may* consist of state staff, but they must not be staff that report to the same organizational component as the project. For example, a department's internal audit unit could supply the oversight team. If a department or agency has a Project Management Office (PMO), and the subject project does not report to the PMO, then the PMO could provide the oversight team. These examples are not meant to preclude the possibility of other solutions being found to meet the independence requirement for oversight on low and medium criticality projects, as long as the requirement to recruit the team from outside the organization that manages the project is met. For medium criticality projects, the oversight team will provide its reports to the Agency and department CIO, and for low criticality projects the reports will be provided to the department CIO and project manager.

### Expertise

The members of the oversight team must have experience as participants in and reviewers of similar projects. The team must possess subject matter expertise in project management, procurement (if applicable), risk management, communications and system engineering. This experience shall have been gained on multiple, similar projects. Teams providing oversight for medium and high-level projects must be formerly trained in industry standard project management and system development methodologies.

### Independent Oversight Activities

The independent oversight process consists of three main components:

1. Review and assessment
2. Reporting
3. Tracking

The oversight team shall conduct reviews for compliance with the Finance “Minimum Requirements for Project Management Practices and Processes” (Appendix A). Templates that may be used in completing the review and assessment are included as Appendix F. There is a separate template for each level of project criticality (low, medium and high).

For each item on the template, the oversight team shall identify the document(s) or other project products that demonstrate performance of the required functions. The team must review and assess the identified items for completeness, currency, comprehensiveness, accuracy and any other attributes pertaining to their quality and appropriateness for their intended function. The template should be employed as a checklist, with the team noting the result of the assessment and the principle sources of input to the assessment process. For any item found to be deficient, the deficiency must be documented separately as a finding within the oversight team’s written report. Agencies may require additional oversight reporting, beyond that required by this framework. The documentation of additional information beyond that included in Appendix G may be added as a supplemental document to the standard reporting format.

### Reporting

The independent oversight team shall compile and report its results in writing, following the format of the Project Oversight Report included as Appendix G. This report replaces the previous monthly project status report required for Control Agency reporting by the Department of Information Technology. In addition to reporting on compliance with the Finance “Minimum Expected Project Management Products and Processes,” the team shall report on any other material findings, conclusions and recommendations made as a result of the review and assessment. Such findings could include, for example, identification of risks, issues, lessons learned, best practices or performance exceeding minimum requirements.

The oversight team shall provide its reports to management regularly at a frequency depending upon project criticality. Reporting requirements are shown in Table 6.1 on the next page.

Table 6.1: Destination and Frequency of Independent Project Oversight Reports

		Project Criticality		
		Low	Medium	High
Oversight report to:		Department	Department/Agency	Department/Agency/Finance
Reporting at least:		Quarterly	Quarterly	Monthly

Tracking

Independent project oversight is a process that begins immediately following project approval and continues through project closeout. The deficiencies, issues, findings and recommendations identified by the oversight process must be incorporated into the appropriate project management processes (e.g. planning and tracking, risk management, etc.). As the project progresses, the review and assessment process must also track the disposition of the team’s prior findings, recommendations and identified deficiencies. Oversight reporting must include follow-up information on the project’s corrective action and implementation of oversight recommendations.

**This Page Intentionally Left Blank**

## Appendix A: Required Project Management Practices and Products

	Low	Medium	High
Planning and Tracking	Formal identification of the project business case, project goals, objectives, expected outcomes, key stakeholders, sponsor(s), etc. (i.e. project charter)	Formal identification of the project business case, project goals, objectives, expected outcomes, key stakeholders, sponsor(s), etc. (i.e. project charter)	Formal identification of the project business case, project goals, objectives, expected outcomes, key stakeholders, sponsor(s), etc. (i.e. project charter)
	Development and maintenance of a project work plan including identification of activities, milestones and schedule	Detailed project planning with all activities (tasks), milestones, dates and estimated hours by task loaded to project management software; lowest level tasks of short duration with measurable outcomes	Detailed project planning with all activities (tasks), milestones, dates and estimated hours by task loaded to project management software; lowest level tasks of short duration with measurable outcomes
		Completion of planned tasks recorded within PM software	Completion of planned tasks recorded within PM software
		Actual hours expended by task recorded at least monthly within PM software	Actual hours expended by task recorded at least monthly within PM software
		Estimated hours to complete by task recorded at least monthly within PM software	Estimated hours to complete by task recorded at least monthly within PM software
	Development and maintenance of a project organization chart	Development and maintenance of a project organization chart	Formal staff planning, including organization chart, written roles and responsibilities, plans for staff acquisition, schedule for arrival and departure of specific staff, and staff training plans
	Development and maintenance of project cost estimates and supporting data for each cost category	Development and maintenance of project cost estimates and supporting data for each cost category	Development and maintenance of project cost estimates and supporting data for each cost category

	Low	Medium	High
Planning & Tracking (cont.)		Use of formal software size estimation where custom software development or COTS modifications are a significant component of cost	Use of formal software size estimation where custom software development or COTS modifications are a significant component of cost
		Use of two or more estimation approaches (e.g. top-down, bottom-up, parametric) to refine estimates	Use of two or more estimation approaches (e.g. top-down, bottom-up, parametric) to refine estimates
			Independent review of estimates
	Recording of actual costs by cost category and comparing actual costs to budget	Recording of actual costs by cost category and comparing actual costs to budget	Recording of actual costs by cost category and comparing actual costs to budget
	Maintenance of supporting data for actual costs	Maintenance of supporting data for actual costs	Maintenance of supporting data for actual costs
	Tracking and reporting (within status reporting process) of work plan activities, schedule and milestone completion status	Tracking and reporting (within status reporting process) of work plan activities, resource utilization, schedule and milestone completion status	Tracking and reporting (within status reporting process) of work plan activities, resource utilization, schedule and milestone completion status
	Change control/approval for key specification documents (e.g. contracts, requirement specifications and other contract deliverables) and software products	Change control/approval for key specification documents (e.g. contracts, requirement specifications and/or contract deliverables) and software products	Formal configuration control, including a written configuration management plan covering change control/approval for key specification documents (e.g. contracts, requirement specifications and/or contract deliverables) and software products and specific staff roles and responsibilities for configuration management.

	Low	Medium	High
Planning and Tracking (cont.)	Tracking of issues/problems and their resolution	Formal tracking of issues/problems and their resolution, including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities	Formal tracking of issues/problems and their resolution, including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities
	Assessment of user satisfaction at key milestones	Assessment of user satisfaction at key milestones	Assessment of user satisfaction at key milestones
		Completion of planned tasks recorded within project management software	Completion of planned tasks recorded within project management software
			Planning in compliance with formal standards or system development life-cycle (SDLC) methodology
			Formal enterprise architecture planning
	Project closeout activities, including a PIER, collecting and archiving up-to-date project records and identifying lessons learned	Project closeout activities, including a PIER, collecting and archiving up-to-date project records and identifying lessons learned	Project closeout activities, including a PIER, collecting and archiving up-to-date project records and identifying lessons learned
Procurement	Use of appropriate procurement vehicle	Use of appropriate procurement vehicle	Use of appropriate procurement vehicle
	Inclusion of a detailed written scope of work for services requested in solicitation document	Inclusion of a detailed written scope of work for services requested in solicitation document	Inclusion of a detailed written scope of work for services requested in solicitation document
		Detailed requirements specifications included in solicitation document	Detailed requirements specifications included in solicitation document
			Material participation of outside expertise (e.g. DGS, Departmental specialists, consultants)

	Low	Medium	High
Procurement (cont.)			Consultation with qualified legal counsel for procurement if outsourcing
Risk Management	Identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines	Identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines	Formal continuous risk management, including development of a written risk management plan, identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines, and regular management team review of risks and mitigation progress
			Use of SEI "Taxonomy Based Questionnaire" or similar risk identification aid(s)
Communications	Regular status reporting to key stakeholders, including progress against timeline and budget; risk management results and status; issue management results and status	Formal communications management, including a written project communications plan. Regular status reporting to key stakeholders, including progress against timeline and budget; risk management results and status; issue management results and status; written escalation policy for issues and risks. Regular stakeholder involvement in major project decisions, issue resolution and risk mitigation	Formal communications management, including a written project communications plan. Regular status reporting to key stakeholders, including progress against timeline and budget; risk management results and status; issue management results and status; written escalation policy for issues and risks. Regular stakeholder involvement in major project decisions, issue resolution and risk mitigation
System Engineering		Ongoing user involvement	Ongoing user involvement
	Formal user approval/sign-off on written specifications	Formal user approval/sign-off on written specifications	Formal user approval/sign-off on written specifications
		Adherence to a formal system development life-cycle (SDLC) methodology	Adherence to a formal system development life-cycle (SDLC) methodology

	Low	Medium	High
System Engineering (cont.)		Tracking requirements traceability through life-cycle phases	Use of requirements management software and tracking of requirements traceability through life-cycle phases
		Adherence to software engineering standards	Adherence to software engineering standards
		Software defect tracking beginning with unit testing	Product defect tracking beginning with requirements specifications
		Performance of formal code reviews	Performance of formal code reviews
		Formal quality assurance through all life-cycle phases	Formal quality assurance through all life-cycle phases
	Formal testing and user sign-off of test results and completed system	Formal testing and user sign-off of test results and completed system	Formal testing and user sign-off of test results and completed system
			Adherence to an enterprise architecture plan
			Deliverable inspections, beginning with requirements specifications
			Formal IV&V

**This Page Intentionally Left Blank**

## Appendix B: Department Project Management Assessment Form

Use the following form to complete the practices and processes section of the department level project management capabilities assessment. (Following is for a low criticality project).

Project Management Capability Assessment: Low Criticality Projects

Activity	All	Some	None
<b>Planning and Tracking</b>			
Are business cases, project goals, objectives, expected outcomes, key stakeholders and sponsor(s) identified and documented?			
Are project work plans including identification of activities, deliverables, milestones and schedule prepared and maintained?			
Are project organization charts prepared and kept current?			
Are project cost estimates, with supporting data for each cost category, maintained?			
Are actual costs, recorded for each cost category, recorded as they are incurred?			
Are actual costs regularly compared to budgeted costs?			
Is supporting data maintained for actual costs?			
Is completion status of work plan activities, deliverables, and milestones recorded, compared to schedule and included in a written status reporting process?			
Is there formal change control/approval for key specification documents (e.g. contracts, requirement specifications and other contract deliverables) and software products?			
Are issues and problems identified and tracked to closure?			
Is user satisfaction assessed at key points in the project?			
Are project closeout activities performed, including completion of a PIER, collection and archiving up-to-date project records and identification of lessons learned?			
<b>Procurement</b>			
Are appropriate procurement vehicles selected (e.g. CMAS, MSA, "alternative procurement") and their required processes followed?			
Is a detailed written contractor scope of work included in solicitation documents?			
<b>Risk Management</b>			
Are risks identified, analyzed, mitigated and escalated in accordance with DOF/TOSU requirements?			

Activity	All	Some	None
<b>Communications</b>			
Are regular written status reports prepared and provided to key stakeholders?			
Do status reports include progress against timeline and budget?			
Do status reports include results and status on risk and issue management?			
<b>System Engineering</b>			
Do users formally approve/sign-off on written specifications?			
Do users sign-off on acceptance test results before a new system is put into production?			

Use the following form to complete the practices and processes section of the department level project management capabilities assessment. (Following is for a medium criticality project).

Project Management Capability Assessment: Medium Criticality Projects

Activity	All	Some	None
<b>Planning and Tracking</b>			
Are business cases, project goals, objectives, expected outcomes, key stakeholders and sponsor(s) identified and documented?			
Are detailed project plans with all activities (tasks), milestones, dates and estimated hours by task loaded to project management software? Are the lowest level tasks of a short duration with measurable outcomes?			
Is the completion of planned tasks recorded within the PM software?			
Are actual hours expended by task recorded at least monthly within PM software?			
Are estimated hours to complete by task recorded at least monthly within PM software?			
Is a project organization chart prepared and kept current?			
Are project cost estimates, with supporting data for each cost category, being maintained?			
Are software size estimates developed and tracked?			
Are at least two software size estimation approaches used?			
Are actual costs recorded as they are incurred for each cost category?			
Are actual costs regularly compared to budgeted costs?			
Is supporting data maintained for actual costs?			
Is completion status of work plan activities, deliverables, and milestones recorded, compared to schedule and included in a written status reporting process?			
Are change control/approval procedures in place for key specification documents (e.g. contracts, requirement specifications and other contract deliverables) and software products?			
Are issues/problems and their resolution (including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities), formally tracked?			
Is user satisfaction assessed at key project milestones?			
Are project closeout activities performed, including completion of a PIER, collection and archiving up-to-date project records and identification of lessons learned?			

Activity	All	Some	None
<b>Procurement</b>			
Are appropriate procurement vehicles selected (e.g. CMAS, MSA, "alternative procurement") and their required processes followed?			
Is a detailed written scope of work for all services included in solicitation documents?			
Are detailed requirement specifications included in solicitation documents?			
<b>Risk Management</b>			
Are risks identified, analyzed, mitigated and escalated in accordance with DOF/TOSU requirements?			
<b>Communication</b>			
Is there a written project communications plan?			
Are regular written status reports prepared and provided to the project manager, department CIO (if applicable) and other key stakeholders?			
Are there written escalation policies for issues and risks?			
Is there regular stakeholder involvement in major project decisions, issue resolution and risk mitigation?			
<b>System Engineering</b>			
Are users involved throughout the project, especially in requirements specification and testing?			
Do users formally approve/sign-off on written specifications?			
Is a formal system development life-cycle (SDLC) methodology followed?			
Are functional and performance requirements traceable through the life-cycle phases?			
Are software engineering standards adhered to?			
Does software defect tracking beginning no later than unit testing?			
Are there formal code reviews?			
Are formal quality assurance procedures followed consistently through all life-cycle phases?			
Do users sign-off on acceptance test results before a new system is put into production?			

Use the following form to complete the practices and processes section of the department level project management capabilities assessment. (Following is for a high criticality project).

Project Management Capability Assessment: High Criticality Projects

Activity	All	Some	None
<b>Planning and Tracking</b>			
Are business cases, project goals, objectives, expected outcomes, key stakeholders and sponsor(s) identified and documented?			
Are detailed project plans with all activities (tasks), milestones, dates and estimated hours by task loaded into project management software? Are the lowest level tasks of a short duration with measurable outcomes?			
Is completion of planned tasks recorded within project management software?			
Are actual hours expended by task recorded at least monthly within PM software?			
Are estimated hours to complete by task recorded at least monthly within PM software?			
Is a project organization chart prepared and kept current?			
Are there procedures for formal staff planning, including written roles and responsibilities, plans for staff acquisition, schedule for arrival and departure of specific staff, and staff training plans			
Have project cost estimates, with supporting data for each cost category, been maintained?			
Are software size estimates developed and tracked?			
Are at least two software size estimation approaches used?			
Are independent reviews of estimates conducted?			
Are actual costs for each cost category recorded as they are incurred?			
Are actual costs regularly compared to budgeted costs?			
Is supporting data maintained for actual costs?			
Is completion status of work plan activities, deliverables, and milestones recorded, compared to schedule and included in a written status reporting process?			
Is formal configuration control practiced, including a written configuration management plan covering change control/approval for key specification documents (e.g. contracts, requirement specifications and/or contract deliverables) and software products and specific staff roles and responsibilities for configuration management?			
Are issues/problems and their resolution (including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities), formally tracked?			

Activity	All	Some	None
Is user satisfaction assessed at key project milestones?			
Is planning in compliance with formal standards or a system development life-cycle (SDLC) methodology?			
Is there formal enterprise architecture planning?			
Are project closeout activities performed, including completion of a PIER, collection and archiving up-to-date project records and identification of lessons learned?			
<b>Procurement</b>			
Are appropriate procurement vehicles selected (e.g. CMAS, MSA, "alternative procurement") and their required processes followed?			
Is a detailed written scope of work for all services included in solicitation documents?			
Are detailed requirement specifications included in solicitation documents?			
Is there Material participation of outside expertise (e.g. DGS, Departmental specialists, consultants) in procurement planning and execution?			
For large-scale outsourcing, is qualified legal counsel obtained?			
<b>Risk Management</b>			
Is formal continuous risk management performed, including development of a written risk management plan, identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines, and regular management team review of risks and mitigation progress performed?			
Does the management team review risks and mitigation progress at least monthly?			
Are externally developed risk identification aids used, such as the SEI "Taxonomy Based Questionnaire?"			
<b>Communication</b>			
Is there a written project communications plan?			
Are regular written status reports prepared and provided to the project manager, department CIO (if applicable) and other key stakeholders?			
Are there written escalation policies for issues and risks?			
Is there regular stakeholder involvement in major project decisions, issue resolution and risk mitigation?			
<b>System Engineering</b>			
Are users involved throughout the project, especially in requirements specification and testing?			

Activity	All	Some	None
Do users formally approve/sign-off on written specifications?			
Is a formal system development life-cycle (SDLC) methodology followed?			
Is a software product used to assist in managing requirements? Is there tracking of requirements traceability through all life-cycle phases?			
Are software engineering standards adhered to?			
Does software defect tracking begin no later than requirements specifications?			
Are there formal code reviews?			
Are formal quality assurance procedures followed consistently through all life-cycle phases?			
Do users sign-off on acceptance test results before a new system is put into production?			
Is the enterprise architecture plan adhered to?			
Are formal deliverable inspections performed, beginning with requirements specifications?			
Are IV&V services used?			

**This Page Intentionally Left Blank**

## Appendix C: Categories and Examples of Risk

### Plan/Schedule

- Schedule is optimistic, "best case," rather than realistic, "expected case"
- Plan omits necessary tasks
- Schedule was based on the use of specific team members, but those team members were not available
- Cannot build a product of the size specified in the time allocated
- Product is larger than estimated (in lines of code, function points, or percentage of previous project's size)
- Effort is greater than estimated (per line of code, function point, module, etc.)
- Re-estimation in response to schedule slips does not occur, or is overly optimistic or ignores project history
- Excessive schedule pressure
- A delay in one task causes cascading delays in dependent tasks
- Unfamiliar or complex areas of the product take more time than expected to design and implement

### Organization and Management

- Project lacks an effective top-management sponsor
- Layoffs and cutbacks reduce team's capacity
- Inefficient team structure reduces productivity
- Lack of specific technical expertise
- Management review/decision cycle is slower than expected
- Budget cuts
- Non-technical third-party tasks take longer than expected (control agency approvals, procurement, equipment purchase, legal reviews, etc.)
- Project plans are abandoned under pressure
- Inaccurate status reporting

#### Development Environment

- Facilities are not available on time
- Facilities are available but inadequate (e.g., no phones, network wiring, furniture, office supplies, etc.)
- Facilities are crowded, noisy, or disruptive
- Development tools are not in place by the desired time
- Development tools do not work as expected; developers need time to create workarounds or to switch to new tools
- Developers unfamiliar with development tools
- Development tools do not provide the planned productivity
- Development environment structure, policies, procedures are not clearly defined

#### User Involvement

- User introduces new requirements after agreed upon requirements specification is complete
- User finds product to be unsatisfactory
- User does not buy into the project and consequently does not provide needed support
- User input is not successfully solicited
- User review/decision cycles for plans, prototypes, and specifications are slower than expected
- User will not participate in review cycles for plans, prototypes, and specifications or is incapable of doing so
- User communication time (e.g., time to answer requirements-clarification questions) is slower than expected
- User-mandated support tools and environments are incompatible, have poor performance, or have inadequate functionality
- User has expectations for development speed that developers cannot meet

#### Contractor Performance

- Contractor does not deliver components when promised
- Contractor delivers components of unacceptably low quality, and time must be added to improve quality
- Contractor does not provide the level of domain expertise needed
- Contractor does not provide the level of technical expertise needed

#### Requirements Management

- Requirements have been base lined but continue to change
- Requirements are poorly defined, and further definition expands the scope of the project
- Additional requirements are added
- Vaguely specified areas of the product are more time-consuming than expected

#### Product Characteristics

- Error-prone modules require more testing, design, and implementation work than expected
- Unacceptably low quality requires more testing, design, and implementation work to correct than expected
- Development of flawed software functions requires redesign and implementation
- Development of flawed user interface results in redesign and implementation
- Development of extra software functions that are not required extends the schedule
- Meeting product's size or speed constraints requires more time than expected, including time for redesign and re-implementation
- Requirements for interfacing with other systems, other complex systems, or other systems that are not under the team's control result in unforeseen design, implementation, and testing
- Requirement to operate under multiple operating systems takes longer to satisfy than expected
- Development in an unfamiliar or unproved software environment
- Development in an unfamiliar or unproved hardware environment
- Dependency on a technology that is new or still under development

#### External Environment

- Product depends on law, policy or regulations that change frequently
- Multiple stakeholders outside the normal department chain of command
- Key software or hardware components become unavailable, unsupported or are unexpectedly scheduled for de-support

#### Personnel

- Acquisition of required project staff takes longer than expected
- Task prerequisites (e.g., training, completion of other projects) cannot be completed on time

- Poor relationships between project team and users or other stakeholders slow decision making and follow through
- Lack of needed specialization (includes technical and domain knowledge) increases defects and rework
- Personnel need extra time to learn unfamiliar software tools or environment
- Personnel need extra time to learn unfamiliar hardware environment
- Personnel need extra time to learn unfamiliar software language
- Unplanned turnover of contractor key personnel
- Unplanned turnover of State key personnel
- New development personnel are added late in the project, and additional training and communications overhead reduces existing team members' effectiveness
- Conflicts between team members
- Problem team members are not removed from the team
- The personnel most qualified to work on the project are not available or are not used
- Personnel with critical skills needed for the project cannot be found
- Key personnel are available only part time
- Not enough personnel are available for the project
- People's assignments do not match their strengths

#### Design and Implementation

- Design fails to address major issues
- Design requires unnecessary and unproductive implementation overhead
- Flawed design
- Use of unfamiliar methodology
- Necessary functionality cannot be implemented using the selected methods and tools
- Schedule savings from productivity enhancing tools are overestimated
- Components developed separately cannot be integrated easily
- Data conversion activities are underestimated or are ignored

Process

- Inaccurate progress tracking
- Upstream quality-assurance activities are limited or cut short
- Poor quality assurance
- Too little formality (lack of adherence to software policies and standards)
- Too much formality (bureaucratic adherence to software policies and standards)
- Weak risk management fails to detect major project risks
- Project management and tracking consumes more resources than expected

**This Page Intentionally Left Blank**

## Appendix D: Project Risk List

Project: \_\_\_\_\_

Date: \_\_\_\_\_

Brief Description of Risk	Impact	Probability	Time	Exposure	Severity
Plan/Schedule					
Organization and Management					
Development Environment					
User Involvement					
Contractor Performance					
Requirements Management					
Product Characteristics					
External Environment					
Personnel					
Design and Implementation					
Management Processes					
Other					

**This Page Intentionally Left Blank**

## Appendix E: Risk Management Form

Risk Management Form		
Probability:	Project:	
Impact:	Risk Title:	
Time Frame:	Originator:	Origination Date:
Severity:	Assigned to:	Report Date:
Risk Assessment		
Risk Statement:		
Risk Context/Analysis:		
Risk Planning		
Strategy: <input type="checkbox"/> Research <input type="checkbox"/> Accept <input type="checkbox"/> Mitigate <input type="checkbox"/> Watch	Action Items	
Risk Tracking		
Event/Action/Commitment:		
Risk Resolution		
Sign-off:	Sign-off:	Sign-off:
Sign-off Date:	Sign-off Date:	Sign-off Date:

**This Page Intentionally Left Blank**

## Appendix F: Project Oversight Review Checklist

### Project Oversight Review Checklist: Low Criticality Project

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
<b>Planning and Tracking</b>			
Have the business case, project goals, objectives, expected outcomes, key stakeholders and sponsor(s) been identified and documented?			
Has a detailed project work plan including specification of activities, deliverables, milestones and schedule been prepared?			
Is there a current project organization chart?			
Are project cost estimates, with supporting data for each cost category, maintained?			
Are actual costs recorded for each cost category recorded as they are incurred?			
Are actual costs regularly compared to budgeted costs?			
Is supporting data maintained for actual costs?			
Is completion status of work plan activities, deliverables, and milestones recorded, compared to schedule and included in a written status reporting process?			
Are change control/approval procedures in place for key specification documents (e.g. contracts, requirement specifications and other contract deliverables) and software products?			
Are issues/problems and their status and resolution tracked from identification to resolution?			

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
Is user satisfaction assessed at key project milestones?			
Are project closeout activities performed, including completion of a PIER, collection and archiving up-to-date project records and identification of lessons learned?			
<b>Procurement</b>			
Has an appropriate procurement vehicle been selected (e.g. CMAS, MSA, "alternative procurement") and the required processes followed?			
Is a detailed written contractor scope of work included in the solicitation document?			
<b>Risk Management</b>			
Are the identification, analysis, mitigation and escalation of risks performed in accordance with DOF/TOSU Guidelines?			
<b>Communication</b>			
Is project status reported regularly to key stakeholders, including progress against timeline and budget, risk management results and status, issue management results and status?			
<b>System Engineering</b>			
Do users formally approve/sign-off on written specifications?			
Is formal testing performed, including user sign-off?			

Project Oversight Review Checklist: Medium Criticality Project

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
Planning & Tracking			
Have the business case, project goals, objectives, expected outcomes, key stakeholders and sponsor(s) identified and documented?			
Has a detailed project plan with all activities (tasks), milestones, dates and estimated hours by task loaded into project management (PM) software? Are the lowest level tasks of a short duration with measurable outcomes?			
Is completion of planned tasks recorded within the PM software?			
Are actual hours expended by task recorded at least monthly within PM software?			
Are estimated hours to complete by task recorded at least monthly within PM software?			
Is there a current project organization chart?			
Have project cost estimates, with supporting data for each cost category, been maintained?			
Are software size estimates developed and tracked?			
Are two or more estimation approaches used to refine estimates?			
Are actual costs recorded and regularly compared to budgeted costs?			
Is supporting data maintained for actual costs?			

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
Is completion status of work plan activities, deliverables, and milestones recorded, compared to schedule and included in a written status reporting process?			
Are change control/approval procedures in place for key specification documents (e.g. contracts, requirement specifications and other contract deliverables) and software products?			
Are issues/problems and their resolution (including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities), formally tracked?			
Is user satisfaction assessed at key project milestones?			
Are project closeout activities performed, including a PIER, collection and archiving up-to-date project records and identification of lessons learned?			
<b>Procurement</b>			
Are appropriate procurement vehicles selected (e.g. CMAS, MSA, "alternative procurement") and their required processes followed?			
Is a detailed written contractor scope of work included in the solicitation document?			
Are detailed requirement specifications included in solicitation documents?			
<b>Risk Management</b>			
Are the identification, analysis, mitigation and escalation of risks performed in accordance with DOF/TOSU Guidelines?			
<b>Communication</b>			
Is there a written project communications plan?			

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
Are regular written status reports prepared and provided to the project manager, department CIO (if applicable) and other key stakeholders?			
Are there written escalation policies for issues and risks?			
Is there regular stakeholder involvement in major project decisions, issue resolution and risk mitigation?			
<b>System Engineering</b>			
Are users involved throughout the project, especially in requirements specification and testing?			
Do users formally approve/sign-off on written specifications?			
Is a formal system development life-cycle (SDLC) methodology followed?			
Is requirements traceability tracked through all life-cycle phases?			
Do software engineering standards exist and are they followed?			
Does software defect tracking begin no later than unit testing?			
Are formal code reviews conducted?			
Are formal quality assurance procedures followed consistently?			
Do users sign-off on acceptance test results before a new system or changes are put into production?			

Project Oversight Review Checklist: High Criticality Project

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
<b>Planning and Tracking</b>			
Have the business case, project goals, objectives, expected outcomes, key stakeholders, and sponsor(s) identified and documented?			
Has a detailed project plan with all activities (tasks), milestones, dates, and estimated hours by task loaded into project management (PM) software? Are the lowest level tasks of a short duration with measurable outcomes?			
Is completion of planned tasks recorded within the PM software?			
Are actual hours expended by task recorded at least monthly within PM software?			
Are estimated hours to complete by task recorded at least monthly within PM software?			
Is there a formal staffing plan, including a current organization chart, written roles and responsibilities, plans for staff acquisition, schedule for arrival and departure of specific staff, and staff training plans			
Have project cost estimates, with supporting data for each cost category, been maintained?			
Are software size estimates developed and tracked?			
Are two or more estimation approaches used to refine estimates?			
Are independent reviews of estimates conducted?			
Are actual costs recorded and regularly compared to budgeted costs?			

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
Is supporting data maintained for actual costs?			
Is completion status of work plan activities, deliverables, and milestones recorded, compared to schedule and included in a written status reporting process?			
Are key specification documents (e.g. contracts, requirement specifications and/or contract deliverables) and software products under formal configuration control, with items to be controlled and specific staff roles and responsibilities for configuration management identified in a configuration management plan?			
Are issues/problems and their resolution (including assignment of specific staff responsibility for issue resolution and specific deadlines for completion of resolution activities), formally tracked?			
Is user satisfaction assessed at key project milestones?			
Is planning in compliance with formal standards or a system development life-cycle (SDLC) methodology?			
Is there a formal enterprise architecture in place?			
Are project closeout activities performed, including a PIER, collection and archiving up-to-date project records and identification of lessons learned?			
<b>Procurement</b>			
Are appropriate procurement vehicles selected (e.g. CMAS, MSA, "alternative procurement") and their required processes followed?			
Is a detailed written scope of work for all services included in solicitation documents?			
Are detailed requirement specifications included in solicitation documents?			

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
Is there material participation of outside expertise (e.g. DGS, Departmental specialists, consultants) in procurement planning and execution?			
For large-scale outsourcing, is qualified legal counsel obtained?			
<b>Risk Management</b>			
Is formal continuous risk management performed, including development of a written risk management plan, identification, analysis, mitigation and escalation of risks in accordance with DOF/TOSU Guidelines, and regular management team review of risks and mitigation progress performed?			
Does the management team review risks and mitigation progress at least monthly?			
Are externally developed risk identification aids used, such as the SEI "Taxonomy Based Questionnaire?"			
<b>Communication</b>			
Is there a written project communications plan?			
Are regular written status reports prepared and provided to the project manager, department CIO (if applicable) and other key stakeholders?			
Are there written escalation policies for issues and risks?			
Is there regular stakeholder involvement in major project decisions, issue resolution and risk mitigation?			
<b>System Engineering</b>			
Are users involved throughout the project, especially in requirements specification and testing?			

Practices and Products	Adequate	Deficient	Notes: Items Reviewed; Interviews Conducted; Demonstration
Do users formally approve/sign-off on written specifications?			
Is a formal system development life-cycle (SDLC) methodology followed?			
Is a software product used to assist in managing requirements? Is the tracking of requirements traceability performed through all life-cycle phases?			
Do software engineering standards exist and are they followed?			
Does product defect tracking begin no later than requirements specifications?			
Are formal code reviews conducted?			
Are formal quality assurance procedures followed consistently?			
Do users sign-off on acceptance test results before a new system or changes are put into production?			
Is the enterprise architecture plan adhered to?			
Are formal deliverable inspections performed, beginning with requirements specifications?			
Are IV&V services obtained and used?			

**This Page Intentionally Left Blank**

## Appendix G: Independent Project Oversight Report

[See separate instruction sheet for guidance on any of the fields in the form]

Project Name: \_\_\_\_\_ Assessment Date: \_\_\_\_\_  
Frequency: \_\_\_\_\_

### Oversight Provider Information

Oversight Leader: \_\_\_\_\_ Organization: \_\_\_\_\_  
Phone Number: \_\_\_\_\_ Email: \_\_\_\_\_

### Project Information

Project Number: \_\_\_\_\_ Department: \_\_\_\_\_  
Criticality: \_\_\_\_\_ Agency: \_\_\_\_\_  
Last Approved Document/Date: \_\_\_\_\_ Total One-time Cost: \_\_\_\_\_  
Start Date: \_\_\_\_\_ End Date: \_\_\_\_\_  
Project Manager: \_\_\_\_\_ Organization: \_\_\_\_\_  
Phone Number: \_\_\_\_\_ Email: \_\_\_\_\_

Summary: Current Status – If multiple current phases, use section at end to assess the status of additional phases.

Project Phase: \_\_\_\_\_  
Planned Start Date: \_\_\_\_\_ Planned End Date: \_\_\_\_\_  
Actual Start Date: \_\_\_\_\_

### Schedule

Select the statement that most closely applies, measured against the last **Finance approved** document.

**Ahead-of-schedule:**

One or more major tasks or milestones have been completed and approved early (> 5%). All other major tasks and milestones completed and approved according to plan.

**On-schedule:**

All major tasks and milestones have been completed and approved according to plan. (Within 5%)

**Behind Schedule:**

One or more major tasks or milestones are expected to be delayed. (> 5%)

Comments: \_\_\_\_\_

Resources (Level of Effort) Choose the statement that most closely applies.

**Fewer Resources**

Completion of one or more major tasks and/or acceptable products has required or is expected to require materially (>5%) fewer hours/staff than planned.

**Within Resources**

All major tasks have been completed and acceptable products created using the planned number of hours/staff (within 5%).

**More Resources**

Completion of major tasks and/or acceptable products has required or is expected to require materially (>5%) more hours/staff than planned.

**Comments:**

Resources (Budget/Cost) Choose the statement that most closely applies.

**Less cost**

The project is (>5%) under budget.

**Within cost**

The project is operating within budget.

**Higher cost**

Material budget increases (>5%) are likely.

**Comments:**

Quality (Client Functionality) Choose the statement that most closely applies.

**Adequately Defined**

Required client functionality is adequately defined, and is being successfully built into the system, given the current project phase.

**Inadequately Defined**

One or more significant components of required client functionality are inadequately defined, or are not being successfully built into the system, given the current project phase.

**Comments:**

Quality (Architecture/System Performance) Choose the statement that most closely applies.

**Adequately Defined**

The system technical architecture is adequately defined, and modeling, benchmarking and testing are being conducted (or are planned) appropriate to the current project phase.

**Inadequately Defined**

The system technical architecture is not adequately defined, or modeling, benchmarking and testing are not being conducted (or are planned) appropriate to the current project phase.

**Comments:**

**New Project Risks**

List (in priority order) the most critical risks to completing the project within the approved schedule, budget and scope. See instructions for description of desired format. If more than five risks are to be included, copy and paste as needed.

**Identifier: Risk Statement:**

**Probability: Impact: Timeframe:**

**Related Findings:**

---

**Identifier: Risk Statement:**

**Probability: Impact: Timeframe:**

**Related Findings:**

---

**Identifier: Risk Statement:**

**Probability: Impact: Timeframe:**

**Related Findings:**

---

**Identifier: Risk Statement:**

**Probability: Impact: Timeframe:**

**Related Findings:**

---

**Identifier: Risk Statement:**

**Probability: Impact: Timeframe:**

**Related Findings:**

**Progress Toward Addressing Prior Risks**

List the risks included in the *New Project Risks* section in previous IPORs. Risks are to remain reported in this section until they are closed or no longer critical, with an explanation of the resolution. See instructions for description of desired content. If more than five risks are to be included, copy and paste as needed.

**Identifier: Risk Statement:**

**Status:**

---

---

**Identifier: Risk Statement:**

**Status:**

General Comments

**Summary: Current Status – Additional phases**

**Project Phase:**

**Planned Start Date:**

**Planned End Date:**

**Actual Start Date:**

**Schedule**

Select the statement that most closely applies, measured against the last **Finance approved** document.

**Ahead-of-schedule:**

One or more major tasks or milestones have been completed and approved early (> 5%). All other major tasks and milestones completed and approved according to plan.

**On-schedule:**

All major tasks and milestones have been completed and approved according to plan. (Within 5%)

**Behind Schedule:**

One or more major tasks or milestones are expected to be delayed. (> 5%)

**Comments:**

**Resources (Level of Effort)** Choose the statement that most closely applies.

**Fewer Resources**

Completion of one or more major tasks and/or acceptable products has required or is expected to require materially (>5%) fewer hours/staff than planned.

**Within Resources**

All major tasks have been completed and acceptable products created using the planned number of hours/staff (within 5%).

**More Resources**

Completion of major tasks and/or acceptable products has required or is expected to require materially (>5%) more hours/staff than planned.

**Comments:**

**Resources (Budget/Cost)** Choose the statement that most closely applies.

**Less cost**

The project is (>5%) under budget.

**Within cost**

The project is operating within budget.

**Higher cost**

Material budget increases (>5%) are likely.

**Comments:**

Quality (Client Functionality) Choose the statement that most closely applies.

**Adequately Defined**

Required client functionality is adequately defined, and is being successfully built into the system, given the current project phase.

**Inadequately Defined**

One or more significant components of required client functionality are inadequately defined, or are not being successfully built into the system, given the current project phase.

**Comments:**

Quality (Architecture/System Performance) Choose the statement that most closely applies.

**Adequately Defined**

The system technical architecture is adequately defined, and modeling, benchmarking and testing are being conducted (or are planned) appropriate to the current project phase.

**Inadequately Defined**

The system technical architecture is not adequately defined, or modeling, benchmarking and testing are not being conducted (or are planned) appropriate to the current project phase.

**Comments:**

## Appendix G: Independent Project Oversight Report – *Instructions*

This report must be completed by the independent oversight provider as described in the Department of Finance Information Technology Project Oversight Framework ([Framework](#)). Questions concerning any aspect of the report can be directed to the Technology Oversight and Security Unit manager assigned to the specific department. Assignments can be found on the Department of Finance website at [TIRU-TOSU Staff Assignments](#), or by calling (916) 445-3137.

### REPORT LAYOUT:

The IPOR includes the following sections:

- ❑ Oversight Provider Information
- ❑ Project Information
- ❑ Summary of Current Status
- ❑ Current Project Risks
- ❑ Progress Toward Addressing Prior Risks

Please note that the *Oversight Provider Information*, *Project Information*, and *Summary: Current Status* sections of the form are locked. If the report is unlocked prior to saving the file, re-locking the file will eliminate all previous responses in these Sections. In addition, the spelling/grammar-checking feature is not available while the file is locked.

Enter the name of the project, the month and year of the assessment (final month if a quarterly report), and indicate whether the report frequency is quarterly or monthly.

### Oversight Provider Information

- Oversight Leader:* Person who has the primary responsibility for the oversight information and who DOF would contact first with any questions regarding the report.
- Organization:* Name of Company, State Department, or Agency conducting Project Oversight.
- Phone Number:* Include area code, and extension if applicable.

### Project Information

- Project Number:* Number assigned by Finance, consisting of a four-digit State organization code, followed by the number assigned to the project by Finance at the time of approval. Example: 1234-023
- Department:* Name of State Board, Department, Office, Commission, etc. with primary ownership of the project.
- Criticality:* Project criticality level assigned by Finance for oversight purposes, (High/Medium/Low)
- Agency:* If the organization listed under Department reports to a State Agency, include the appropriate Agency. If not applicable, show “N/A”

*Last Approved Document & Date:* List the last approved project document, for example FSR or SPR, followed by the date the document was approved by Finance. If multiple documents exist of the last approved type, include the sequence number with the type. For example, if a project has had two SPRs, the last being approved by Finance on November 25, 2002, the field would look as follows: SPR2 - 11/25/2002

*Total One-time Cost:* The total one-time cost included in the last Finance approved project document.

*Start/End Dates:* Enter the project start and end dates from the project schedule included in the last Finance approved project document.

*Project Manager & related information:* Enter the individual with the primary responsibility for the project, whether State employee or vendor. If the project manager is a vendor, include the name of the vendor’s company. If the project manager is a State employee, include the Division or Branch in which they work. Include their direct phone number (formatted as previously mentioned) and email address.

Summary: Current Status
-------------------------

*Project Phase:* Show the current phase of the project based on the approved project plan or using the system development life-cycle project phases (for example planning, design, development, or system test). If this is a phased implementation with multiple current phases, use the section at the end of the form to include the required information for the additional current phases.

List the planned starting and ending dates for the project phase, based on the project schedule included in the Finance approved project document. Enter the actual date that the phase began.

*Assessments (Schedule, Resources-effort, Resources-budget, Quality-Client Functionality, and Quality-System Performance)* Using the drop down boxes, choose the assessment for each of the five areas that most closely match the current project status. The first three areas have a plus/minus five percent benchmark. The intent is to obtain the oversight provider’s professional opinion of the current status, knowing that information may not be available to estimate within the five percent parameter (with a great amount of certainty).

If the current status cannot be reasonably determined for a given area, add a comment that describes the situation and the barrier. [Include a comment of “N/A” for any areas that are not applicable to the current phase.] For the Schedule area, status is measured against the timeframes in the last Finance approved document. In the Resources-Budget area, consider the timing of expected expenditures, for example fixed price contracts and hardware/software purchases. The comments field may also be used to clarify why the project is not within the approved project parameters, or to explain the degree to which they differ.

New Project Risks
-------------------

**NOTE:** Only the newly identified, most critical risks will be shown in this section on each report. Risks included in this section on previous reports should be transferred to the *Progress Towards Addressing Prior Risks* section.

*Risk Statement:* List in priority order the new, most critical risks to the project. These should include project risks associated with all categories identified in the Framework, including risks associated with the lack of appropriate project management practices and tools. Please refer to Sections 5, 6, and Appendices B, C and F of the Finance Framework for guidance and examples of appropriate risk statements. Each risk statement should concisely include the three following components: the concern, the likelihood, and one or more potential consequence. Do not limit the number of risks included in the IPOR to the five spaces shown in the template.

*Identifier:* These most critical risks should be a subset of a larger list of risks actively being managed by the project. Many organizations have automated or custom tools to manage project risks which include a risk identifier system that is meaningful to the organization. The IPOR template includes a field for identifier. These should reflect the risk identification system used on the project. It may be sequential numbers or another more sophisticated identification system used by the project. Any method is adequate, as long as consistency is maintained throughout the life of the project, and identifiers are not re-used during the life of a project. Entries made in this section will move to the “Progress toward addressing prior risk/findings” section in subsequent reports. As they are moved, each risk will retain its unique identifier.

*Probability, Impact, & Timeframe ratings:* Rate the *Probability*, *Impact*, and *Timeframe* for each risk. *Probability* and *Impact* choices are High, Medium, and Low. The *Timeframe* options are Long, Medium, and Short. A methodology for determining these factors is included in Section 5 of the Finance Framework.

*Related Findings:* Each risk will have one or more findings to support the risk statement. The finding(s) will explain the probability, impact, and timeframe designations. A finding should include the:

- Condition (what was found),
- Criteria (what was expected), and
- Cause (factors responsible for the difference).

A finding statement should also include the effect, or potential impact of the finding.

### Progress Toward Addressing Prior Risks

All risks included in the *Current Project Risks* section on previous reports must be displayed in this section at least once. If the risk was successfully resolved between the time of inclusion in the prior section and the next report, it must still be included in this section. Risks remain reported in this section until they are closed or no longer critical, with an explanation of the resolution.

- Identifier:* The identifier will not change when moved to this section.
- Risk Statement:* The risk statement from the prior section is typically moved in its entirety to this area. It is possible that one of the parameters changes, for example the timeframe, however the risk remains critical and therefore stays on the list.
- Status:* Describe the current actions taken regarding the risk or the associated findings. This would include mitigation strategies or action plans obtained from the project. If sufficient changes have occurred to render the risk no longer critical, for example the timeframe for the risk has passed, fully explain the change under status, and the risk can be removed on the subsequent report.
- If the project manager disagrees with the risk, as identified by the oversight provider, this should be also noted in the status.

### General Comments

Include any additional information relevant to the project from an oversight perspective beyond the detail provided in the other sections of this report. This could include additional findings (for example positive findings or findings not associated with the most critical risks) or further clarification/background material to the risks shown in the new or prior sections of the report.

### Attachments:

Oversight providers will include a completed *Project Oversight Review Checklist* (Appendix F of the Framework) with the initial IPOR submitted to Finance for each project. Inclusion of the checklist with subsequent reports is optional. Generally, oversight providers are encouraged to attach any additional documents that provide detailed or supporting information, for example the current project schedule, cost sheet, or full project risk list, when submitting an IPOR. At the discretion of TOSU, specific project documents may be required to be submitted with the IPOR.

**This Page Intentionally Left Blank**

## Appendix H: Definition of Terms

Term	Recommended Working Definition
Completed	<p>Joined the project before development.</p> <p>Worked on a project through initial implementation.</p>
COTS Installation	The initial installation of a commercial-off-the-shelf (COTS) package, with or without package supported customization.
Custom Development	The initial development of a custom designed software application.
Custom Update / Upgrade	The updating or upgrading of a custom designed and developed software application. New functionality should be considered Custom Development rather than an update or upgrade.
Data Center / Network Operations Center	The initial installation or subsequent upgrading of data center or network operation operations center hardware items such as a UPS, generator and monitoring center.
Distributed / Enterprise Server	Multiple servers deployed in a distributed fashion in order to locate computing resources closer to de-centralized user base or one or more enterprise servers located centrally at a data center facility.
Enterprise Architecture	A coherent collection of standards, policies and principles that guide the selection, acquisition, implementation, integration and management of IT hardware and software resources.
Hardware	Any physical device used to capture, process, transmit and / or store data.
Infrastructure (Software)	With regard to computer software, the installation, implementation or upgrading of a third party application integration utility such as transaction processing monitor or database management system.
Infrastructure Install / Upgrade	The initial installation or post installation upgrading of IT infrastructure items such as network cabling, network equipment, data center facility hardware (UPS, Generator) or network operations monitoring equipment.
Initial Implementation	First production use.
IV&V	Independent Verification and Validation.
Key Staff	To include staff in leadership roles (Team Leads) and staff bearing significant technical responsibility (DBA, System Architect) that may not be team leads.
Layered Product	A third-party software application utility used to control and / or support the use of a computing platform or software application (Backup software, monitoring utilities)

Term	Recommended Working Definition
Like Project	A project in the same size category, similar degree of complexity, and similar technology as the subject project.
Local Area Network / Cabling	Local Area Network (LAN) communication equipment and / or cabling used to support a single location such as a County Office.
Local desktop / Server	One or more desktop PC's or server devices that are located and operated at a single location such as a County Office.
Metropolitan / Wide Area Network	Metropolitan and / or Wide Area Network (MAN / WAN) communication equipment and circuits.
Middleware	A third-party application integration utility used as part of an overall software application solution (BEA's Tuxedo Transaction Processing Monitor)
New Install	With regard to computer hardware, the initial installation of any computing device(s) in either a local office (desktop or server room) or a data center setting.
Parametric	Parametric analysis employs equations that describe relationships between cost, schedule, and measurable attributes of systems, hardware, and software.
PIER	Post Implementation Evaluation Report.
Project initiation	Beginning of RFP preparation if applicable; or actual start of work if no formal procurement is planned.
SEI "Taxonomy Based Questionnaire"	<p>The SEI "Taxonomy Based Questionnaire" is an industry standard comprehensive IT project risk questionnaire designed to help organize and study the full breadth of potential software technical risk.</p> <p>Visit the following website for additional information:  <a href="http://www.sei.cmu.edu/sei-home.html">http://www.sei.cmu.edu/sei-home.html</a></p>
Software	Instructions that direct hardware to perform desired functions.
Update / Upgrade	With regard to computer hardware, the updating or upgrading of an existing computing device(s). Note that a "forklift" upgrade of a computing device should be classified as a New Install.