



California
TECHNOLOGY AGENCY

IT Risk Mitigation Review

(Assembly Bill 617 Report)

June 30, 2012

June 30, 2012

Dear Senators and Assembly Members,

Assembly Bill 617 (Chapter 736, Statutes of 2007) requires the Department of General Services develop and maintain criteria for the evaluation of risk to the State, including the determination of need for financial protection, resulting from the acquisition of information technology goods or services. The Department of General Services was to then submit the criteria to the Joint Legislative Budget Committee and the State Chief Information Officer by June 1, 2008.

Assembly Bill 617 further requires the Technology Agency (then referred to as Office of the Chief Information Officer) to review and report to the Legislature on all contracts approved in accordance with the established risk analysis criteria, and report to the Legislature any recommendations for changes to Public Contract Code Section 12112 instituting the risk analysis requirement or changes to the criteria developed and maintained.

The Technology Agency respectfully submits this report documenting our review.

Sincerely,



Carlos Ramos
Secretary
California Technology Agency

TABLE OF CONTENTS

EXECUTIVE SUMMARY	4
BACKGROUND.....	6
INTERIM GUIDELINES	6
PERMANENT RISK EVALUATION CRITERIA	7
REVIEW.....	10
RECOMMENDATIONS.....	11
Appendix A – AB 617 (Torricono).....	13

EXECUTIVE SUMMARY

Assembly Bill 617 (Chapter 736, Statutes of 2007) required the Department of General Services, which is responsible for conducting and overseeing the State's procurements for information technology goods and services, to develop and maintain, in consultation with the Department of Finance, criteria for the evaluation of risk in the acquisition of information technology goods or services, and strategies to mitigate that risk.

Assembly Bill 617 (hereafter referred to as AB 617) also required the Department of General Services to submit the criteria to the Joint Legislative Budget Committee and to the State Chief Information Officer (now Technology Agency) by June 1, 2008. (Please see Appendix A for the complete text of AB 617.)

Lastly, AB 617 required the Technology Agency to review and report to the Legislature on all contracts approved pursuant to this law by July 1, 2012 and make recommendations for changes to the law or changes to the criteria developed and maintained by the Department of General Services.

Until the Department of General Services could establish the risk criteria, it developed and published the *Interim Risk Evaluation Guidelines for Information Technology (IT) Goods and Services Contracts (AB 617)*. The Interim Guidelines, which provide for a department's assessment of each IT solicitation based on mission criticality, project value, degree of risk to the State's finances, functions or resources, degree of impact to internal/external environments, and project complexity (skills, knowledge, degree of customization) were published by the Department of General Services in a Broadcast Bulletin on March 19, 2008.

Departments were directed to apply the Interim Guidelines to all projects with solicitations valued at \$1 million or more and departments may apply the criteria to those projects with solicitations valued less than \$1 million. Departments are required to determine the risk level (High, Medium or Low) associated with each project, and based on that level determine the appropriate financial protections to utilize, such as withholds, a performance bond, letter of credit, and liquidated damages.

Subsequent to the publication of the Interim Risk Evaluation Guidelines, the Department of General Services engaged a vendor to develop risk criteria and an automated tool for departments to use to identify and evaluate potential project risks.

In its June 2009 report to the Joint Legislative Budget Committee and the State Chief Information Officer, the Department of General Services endorsed a risk identification and mitigation framework (known as MOPS) and indicated it has a tool that automates the framework so that departments can methodically evaluate risk. The Department of

General Services, however, determined that this framework could result in protests and did not release this framework and associated tool.

The California Technology Agency, pursuant to AB 617, was tasked with reviewing contracts approved on and after January 1, 2008 having used the risk mitigation framework, and reporting to the Legislature any recommendations for changes to the risk mitigation framework developed by the Department of General Services or changes to the law. As the Department of General Services has not yet released the framework for use the Technology Agency cannot determine its value to projects, but has specific recommendations regarding the implementation of a risk mitigation framework, and the law.

BACKGROUND

Prior to AB 617 being signed into law in 2008, statute required contractors to submit a performance bond of not less than 50% of the value of a contract for information technology goods or services for contracts which contained progress payments. Additionally, a ten percent minimum payment withhold from the contract was required until final delivery and acceptance of the goods and services.

AB 617 eliminated these statutory requirements and required that the Department of General Services, in consultation with the Department of Finance, develop and maintain risk evaluation criteria that would help departments determine the appropriate approach to achieve financial protections. The Department of General Services published Interim Risk Evaluation Guidelines in March 2008 for departments to use to identify risk levels and provide guidance on appropriate risk mitigation strategies until the risk criteria were developed.

INTERIM GUIDELINES

The Interim Risk Guidelines defined categories of potential risks associated with the procurement and identified risk protections based on the risk rating determined by the department.

The Department of General Services included these categories of potential risks and a few questions for the departments to consider when determining risk on their projects.

Risk Factor	Questions to Evaluate Risk Level
Mission Criticality	How is the solicitation critical to the success of the department's mission, program or project? Is the purchase connected to public safety and/or welfare? Is the proposed purchase a highly visible, politically-sensitive project or issue?
Value	What are the estimated initial (one-time) and overall, life-cycle costs and value of the project?
Risk	What degree of jeopardy is there to the State's finances, functions or resources and are the potential losses measurable?
Impact	To what degree will the project affect internal and external environments? Are there any legal political and regulatory issues to consider?
Complexity	What level of skills, knowledge, abilities and capacity are needed for the life of the purchase? To what degree is customization expected?

Departments then rate the individual characteristics and any other known unique risks as high, medium, and low, and such rating then drives the identification of the risk mitigation strategies recommended by the Department of General Services. The risk mitigation strategies include withhold of a percent of payments, liquidated damages, performance

bonds, letters of credit, and other forms of security to ensure performance, the values of which are adjusted based on contract or project value and department needs. Specifically, the Interim Risk Criteria Guidelines suggest that, based on the risk rating, a department applies the following risk mitigation strategies:

Total Project Risk Category	Withholds	Liquidated Damages	Performance Bond	Letter of Credit
High and progress payments are provided	10% and either performance bond or letter of credit for their stated values	None	30-50% contract value	150 – 200% contract value
High and no progress payments are provided – one or more of the following	10%	Yes, but no value specified	Yes, but no value specified	Yes, but no value specified
Medium and progress payments are provided	10% and either performance bond or letter of credit for their stated values	Yes, but no value specified	20-30% of contract value	100 – 150% of project value
Medium and no progress payments – one or more of the following	At least 10%	Yes, but no value specified	Yes, but no value specified	Yes, but no value specified
Low	10% (optional)	Consider	Consider	Consider

In all cases, the Department of General Services also included as a risk protection, “Any other form of security or guaranty of performance in an amount and method sufficient to protect the State in case of default by the contractor, or any other breach or malfunction of the IT goods and services.”

The procuring department was then to submit to the Department of General Services Procurement Division Director for approval the chosen risk mitigation strategies.

PERMANENT RISK EVALUATION CRITERIA

While the Interim Risk Criteria Guidelines were published in March 2008, the Department of General Services engaged a vendor to assist it in developing the permanent risk evaluation criteria required by AB 617.

On January 6, 2009 the vendor produced its report. With regard to identifying risk, the vendor provided a comprehensive and thoroughly constructed methodology with specific steps which include:

- Evaluating risk by project phase, acknowledging that risks change by phase
- Engaging many stakeholders in the risk assessment, not just the procuring department and the Department of General Services. These might include the Department of Finance, State Chief Information Officer, oversight evaluator, and independent verification and validation.
- Assessing many risk factors (not just cost) such as whether:
 - it is a custom developed solution
 - there are federal penalties associated with late delivery
 - the project is politically sensitive
 - a legislative mandate drives the need for the project
 - the proposed solution has been used elsewhere
 - the vendor has experience working with multiple external stakeholders
 - the development of the Request for Proposals is a lengthy process
 - the project affects public health and safety
 - the project includes a time and materials contract
- Assigning a score based on answers to specific questions in each of the risk factor categories to determine whether the project is high (rating of 70-100% of total risk score), medium (rating of 31-69%), or low risk (rating of 0-30%)
- Determining impact and probability of occurrence of these risk factors
- Calculating the risk score based on impact and probability values
- Identifying risk mitigation mechanisms based on the risk score.

(Please see Appendix B for the risk factors, and specific questions that would be posed to the procuring department along with an impact evaluation.)

Once the risk rating is determined, the procuring department would apply the risk mitigation mechanisms as identified in the table below:

Total Project Risk Category	Withholds	Limitation of Liability	Liquidated Damages	Fixed Price Deliverables	Performance Bond	Letter of Credit
High	Yes – no minimum amount specified	200% of contract value	Yes – no minimum amount specified	Yes	No	No
Medium	Yes – no minimum amount specified	150% of contract value	Yes – no minimum amount specified	Yes	No	No
Low	Maybe	100% of contract value	No	When appropriate	No	No

The vendor also recommended that DGS capture information on the impact risk mitigation strategies had on the success of the project and use the actual experiences to modify the risk mitigation process based on impact.

In its June 2009 Report to the Legislature entitled, *Criteria to Evaluate Risk Resulting from the acquisition of Information Technology Goods and Services*, the Department of General Services recommended that the risk mitigation mechanisms be applied per the following:

Total Project Risk Category	Withholds	Limitation of Liability	Liquidated Damages	Performance Bond	Letter of Credit
High and progress payments are provided	10-20%	200% of contract value	Yes, but no value specified	Not recommended, but if used 20-50% of FSR estimate of total project costs	Not recommended, but if used 100 – 200% of FSR estimate of total project costs
Medium and progress payments are provided	10%	150% of contract value	Yes but no value specified	Not recommended	Not recommended
Low	10%	100% of contract value	No	Not recommended	Not recommended

In February 2010, DGS issued a report with the same title, and included all of the above risk mitigation strategies, but changed the withhold amounts to the following:

- High and progress payments are provided: 5-20%
- Medium and progress payments are provided: 5-10%
- Low: 3-10%

The Department of General Services indicates in the report that departments will submit their risk mitigation mechanism and rationale for Department of General Services' approval, within the Information Technology Procurement Plan. The Department of General Services indicated in the report that an Internet link to the risk mitigation framework (known as MOPS, comprised of each phase of the analysis: **M**anagement of Projects, **O**rganizational Factors, **P**roject Type, and **S**cope) and its associated automated tool would be in each solicitation document, and available via the Internet.

According to Department of General Services' report, the MOPS framework has been tested and validated to assure that it considers project factors that apply risk and can be mitigated in the project acquisition phase. It will also serve as the repository for data related to

technology projects and the outcomes of those projects vis-à-vis the risk mitigation strategies employed. As a result, the state will have more information related to which mitigation strategies are most effective.

The Department of General Services reported that it would continuously maintain and update the MOPS framework based on data collected from tracked projects. Updating the framework based on implemented projects will result in valuable information, and a more valuable tool.

In the report, the Department of General Services also proposed that the State institute a practice of validating financial stability of all participating bidders as risk criterion for acquisitions with estimated contract values above \$10 million and stated it had a repeatable process for doing so. Additionally, Department of General Services proposed that a bidder's past performance on all technology acquisitions be considered. Lastly, the Department of General Services indicated that it was establishing a pilot to institute this statewide.

REVIEW

When performing the review in preparation to conduct the analysis for this report, the Technology Agency reviewed enabling statute, both reports the Department of General Services submitted to the Legislature, and the "Financial Risk Mitigation Report" developed by the Department of General Services' consultant.

Additionally, the Technology Agency asked the Department of General Services whether the pilot mentioned in its report to validate the risk assessment methodology was undertaken and what the results were. The Department of General Services reported there were no results to analyze at this time.

After issuing its reports, the Department of General Services subsequently determined that using the proposed framework and methodology without changing several questions, answers and weighting factors would render the tool and its resulting recommendations susceptible to bid protest and court challenges which would undermine both the IT Risk Tool and the procurements on which it would be used. As a result, the Department of General Services did not release the proposed framework and associated tool. Instead, the Department of General Services believes that the IT Risk Tool can be used internally by the Procurement Officials and bid evaluation teams to do several things: 1) provide initial assessment of risk factors during the Feasibility Study Report and bid development phase, 2) develop recommendations of risk mitigation measures that should be considered during the bid development phase, 3) be a factor in the assessment of the risk levels presented by the pool of bidders who are responsive to a bid (along with financial assessment of potential bidders), and 4) help establish the range of risk mitigation measures to be used in the evaluation award phase. The Department of General Services is pursuing development of the processes and procedures to put this in place and is just now beginning the process of utilizing the tool with active procurements.

Because the Department of General Services believes the tool—as previously configured—would not produce consistent data or results, they have elected to revise the risk mitigation methodology. The Department of General Services has modified the tool and proposes using a revised methodology which will:

- be designed to assess project risk prior to release of the procurement and bidder risk during the procurement;
- be designed to allow for establishment of a range of risk based on the draft bidder pool;
- allow for setting performance bond levels at the lowest possible and prudent bonding and cost appropriate for the project, based on project risk and draft bidder pool;
- be used in conjunction with a financial evaluation to be performed on each bidder; and
- be implemented initially through the use of a pilot program.

As the Department of General Services is still in the development phase, a variety of tasks still need to be completed before pilot implementation can occur. The Department of General Services indicates that the pilot will be completed between June and December 2013, at which time the Department will be in a position to further report on progress of risk mitigation. If the results are positive, the Department will replace the Interim Risk Guidelines with the newly implemented methodology.

RECOMMENDATIONS

The Technology Agency makes the following recommendations based on its analysis:

1. The Department of General Services should identify the specific shortcomings of the risk mitigation framework developed by its consultant, and how the new plan will address these issues.
2. The Department of General Services should apply the risk mitigation framework and mitigation strategies its consultant developed to 20 projects with the highest project cost that are in the implementation stage to determine what variances in approach the state might have taken. Then the Department of General Services should solicit the affected departments to ask them to determine whether the risk mitigation strategies the tool suggested would have better helped them during project implementation to manage the vendor. This would help establish the validity of the framework.
3. The Department of General Services should take into consideration more than the project or vendor cost as a risk factor when determining risk mitigation strategies.

Its own vendor made and supported a strong case for including more than cost in any risk evaluation methodology.

4. The Department of General Services should vet the methodology it wants to adopt with a variety of stakeholders, including the Department of Finance, the California Technology Agency, state departments, and vendors.
5. The Department of General Services should implement the process to validate financial stability of vendors that was referenced in their original report.
6. The Department of General Services should implement its pilot to capture bidders' past performance.

Appendix A – AB 617 (Torricon)

Assembly Bill No. 617

CHAPTER 736

An act to amend, repeal, and add Section 12112 of the Public Contract Code, relating to public contracts.

[Approved by Governor October 14, 2007. Filed with Secretary of State October 14, 2007.]

Legislative Counsel's Digest

AB 617, Torricon. State contracts: information technology goods and services.

Existing law authorizes the Department of General Services to provide for progress payments in any contract for information technology goods or services that are to be manufactured or performed by the contractor, exclusively for the state, at the contractor's shop or plant, provided that not less than 10% of the contract price be withheld until final delivery and acceptance of the goods or services, and that the contractor submit a faithful performance bond, in a specified sum.

This bill would, until July 1, 2013, delete the performance bond requirement, and would require the department, in consultation with the Department of Finance, to develop and maintain criteria for the evaluation of risk to the state that results from the acquisition of information technology goods or services, and would require this risk analysis to determine the need for financial protection that is in the best interest of the state, as specified. This bill would also require the department to submit the criteria developed and maintained for the evaluation of risk to the state that results from the acquisition of information technology goods and services to the Joint Legislative Budget Committee and to the State Chief Information Officer, as specified. This bill would require the State Chief Information Officer to review all contracts approved pursuant to this provision, as specified, and to submit a report to the Legislature, as specified.

The people of the State of California do enact as follows:

SECTION 1. Section 12112 of the Public Contract Code is amended to read:

12112. (a) Any contract for information technology goods or services, to be manufactured or performed by the contractor especially for the state and not suitable for sale to others in the ordinary course of the contractor's business may provide, on the terms and conditions that the department deems necessary to protect the state's interests, for progress payments for work performed and costs incurred at the contractor's shop or plant, provided that not less than 10 percent of the contract price is required to be withheld until final delivery and acceptance of the goods or services.

(b) The department, in consultation with the Department of Finance, shall develop and maintain criteria for the evaluation of risk to the state that results from the acquisition of information technology. This risk analysis shall determine the need for financial protection that is in the best interest of the state, including, but not limited to, any of the following:

(1) An acceptable performance bond as described in Chapter 2

(commencing with Section 995.010) of Title 14 of Part 2 of the Code of Civil Procedure.

(2) Any surety as defined in Section 2787 of the Civil Code.

(3) A letter of credit as described in Division 5 (commencing with Section 5101) of the Commercial Code.

(4) Protection in the form of contract terms.

(5) Any other form of security or guaranty of performance in an amount sufficient to protect the state in the case of default by the contractor providing information technology, or any other breach or malfunction of the goods or services, or both.

(c) The department shall, on or before June 1, 2008, submit the criteria developed and maintained pursuant to subdivision (b) to the Joint Legislative Budget Committee and to the State Chief Information Officer.

(d) The State Chief Information Officer shall, on or before July 1, 2012, do both of the following:

(1) Review and report to the Legislature on all contracts approved pursuant to this section on and after January 1, 2008.

(2) Report to the Legislature any recommendations for changes to this section or changes to the criteria developed and maintained by the department pursuant to subdivision (b).

(e) For purposes of this section, "information technology" means information technology goods or services, or both, as appropriate.

(f) This section shall become inoperative on July 1, 2013, and shall be repealed on January 1, 2014.

SEC. 2. Section 12112 is added to the Public Contract Code, to read:

12112. (a) Any contract for information technology goods or services, to be manufactured or performed by the contractor especially for the state and not suitable for sale to others in the ordinary course of the contractor's business may provide, on the terms and conditions that the department deems necessary to protect the state's interests, for progress payments for work performed and costs incurred at the contractor's shop or plant, provided that not less than 10 percent of the contract price is required to be withheld until final delivery and acceptance of the goods or services, and provided further, that the contractor is required to submit a faithful performance bond, acceptable to the department, in a sum not less than one-half of the total amount payable under the contract securing the faithful performance of the contract by the contractor.

(b) This section shall become operative on July 1, 2013.

APPENDIX B:

Risk Factor Matrix from Financial Risk Mitigation Report

(Submitted to the Department of General Services on January 6, 2009)

ID	RISK FACTOR	RATIONALE FOR INCLUSION
1	Changing Requirements and Specifications	This typically suggests incomplete or inadequate requirements definition at the onset of the project. This may result from an overly long or extended schedule, key personnel turnover, or a myriad of other influencing factors. Constantly changing requirements and specifications is among the leading factors of why projects fail.
2	COTS (Commercial Off-the-Shelf) Software	Installation of a COTS package requires that the department modify its business practices to some degree to conform to the software. The department must conduct a proper business flow analysis to identify the least amount of business process change that will conform to the COTS and yet still meet the needs of the procuring organization.
3	Custom Development	Custom development requires that the department form an experienced and integrated team, requirements are extremely well documented, and the users are heavily committed to making themselves available to the project team. The requirements for sponsor involvement, project management, and resource availability are typically higher for successful completion of a custom development project. The vendor must have an effective plan for coordinating these resources.
4	Customer-in-Use	The requirement to have a specific software or hardware package in use somewhere else prior to acceptance in a bid for the State of California-current regulation is that the product must be in installed for eight months or six months at time of bid submission-SAM 5203, 5221.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
5	Data Center Support	Projects that require data center support require a high level of coordination and communication to ensure the appropriate support is available. Unanticipated delays in data center support; including procurement, installation, and configuration of hardware and/or software, often has a corresponding impact on the project schedule.
6	External Customers	A significant effort is required to obtain external customer requirements. In addition, effective communication is required to get external customer buy-in to project objectives, goals, and deliverables. For example, external customers include the Feds and other non-CA state agencies.
7	Federal Funded/Penalties	Any delay or improper implementation would cost the state money. Federal funding is normally attached to a regulation or agreement with the State. Lack of compliance with the agreement or meeting the requirements of a regulation can result in penalties.
8	Fully Outsourced New Development Services	This type of project relies on the department's experience and capability to manage this type of contract. Critical to its success is effective is adequately defined requirements and detailed deliverable review and management.
9	Ill-defined or Poor Requirements Definition	This risk factor often indicates the lack of user involvement in the requirements definition process or not following a requirements definition methodology.
10	Inappropriate Development Tools	If the developer is not using appropriate development tools, the project and system are at risk of delays and ultimately failure as these tools may impede the development process. Development tools must match the chosen language, architecture, etc and assist the developer in performing their tasks.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
11	Inappropriate User Documentation	User documentation is usually critical to user understanding of a system, and exploitation of system functionality. Poor user documentation increases the likelihood of user dissatisfaction. User satisfaction is a major measurement of project success
12	Lack of an IT Strategic Plan	As with a technical architecture, an organization needs an IT Strategic Plan to ensure that planned IT systems are supporting business objectives and a set of management-blessed priorities exists about which systems are most important in meeting organizational needs. For example, AIMS or similar document.
13	Lack of Early Involvement of Key Vendor Resources	Key resources include business analysts with knowledge of the requirements, IT personnel who understand how the technical solution might work etc. The project needs both types of contractor personnel in a coordinated effort to ensure project success. Even if the project team recognizes the problem in time to avert failure, at minimum the project is subjected to unplanned rework, schedule delays, or cost overruns.
14	Lack of IT Infrastructure	The organization must factor its IT infrastructure into project planning. The IT infrastructure must be assessed against the technical solution and any risks identified and mitigated as appropriate. For example, adopting a sophisticated technical solution when staff are just learning to use PCs.
15	Lack of Proper Evaluation of IPORs	Oversight Consultants submit monthly IPORs. An appropriate process to review and act on information in IPORs is necessary.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
16	Lack of Vendor Capability to Develop an Appropriate Project Plan	The planning and organization of a project are dependent upon a project plan. Proper project plans are essential to reduce the risk of project failure.
17	Lack of Vendor Capability to Implement Communication Plan	At all times in a project and particularly with a large project team, it is imperative that a thorough communication plan be adopted and followed. Poor communication between department managers, stakeholders, those who build and manage new IT infrastructure and the project team invariably leads to uninformed decisions. One indication of the possibility of poor communication management is lack of a project communication plan. A project communication plan is an excellent device to introduce into a project appropriate processes to ensure effective project communication with all stakeholders.
18	Lack of Vendor Capability to Perform in a Cross Program Environment	Multi-program projects within a department have very particular challenges. It is difficult for department to achieve their objectives, especially when there are competing priorities. A project deemed important by one department or program may unintentionally wind up lower in priority for another department or program. Increasing numbers of cross program involvement increases the likelihood of risk.
19	Lack of Vendor Capability to Perform in Multi-Agency Environment	A significant effort is required to obtain requirements from each agency. Agencies each have their own competing priorities, and if the process requires identification of one as the primary project, the other involved agencies may or may not assign the priority to the project that is necessary to reach successful conclusion. Dispute resolution is especially challenging in a multi-agency project. Increasing numbers of stakeholders involved increases the likelihood of risk.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
20	Lack of Vendor Capability to Perform in Multiple Local Governments or Counties Environment	A significant effort is required to obtain requirements from each local government or county. Each local government may have their own competing priorities, causing prioritization conflict. Dispute resolution is especially challenging in projects that span multiple local governments or counties. Increasing numbers of stakeholders involved increases the likelihood of risk.
21	Lack of Vendor Capability to Provide Appropriate Technical Architecture	An organization that is developing information systems needs to have specified an appropriate technical architecture within which it will develop its information systems and IT services. Without a defined technical architecture, solutions developed often strain resources and create integration problems.
22	Lack of Vendor Capability to Transfer Knowledge to State Staff	If an organization lacks sufficient domain knowledge, the organization must factor it into project planning. This would suggest the project must procure this knowledge from an external resource. For example, a department staff has no experience with the proposed technical architecture; vendor must demonstrate in the proposal capability to transfer knowledge to State staff.
23	Lack of Vendor Management of Statewide Customers	A significant effort is required to obtain statewide customer requirements. In addition, effective communication is required to get external customer buy-in to project objectives, goals, and deliverables. For example, department business units around the state impacted by different environmental factors.
24	Lack of Vendor's PM Infrastructure or Methodology	This may indicate that the vendor and its staff are not ready to assume primary responsibility for execution of more complex projects without outside assistance. Proper assessment of this risk factor requires a technical assessment of the complexity and difficulty of the project and the experience and background of the vendor staff who will manage the project.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
25	Legislative Mandate	Legislative Mandates determine the completion date of the project. If the state does not comply by the mandated completion date, then penalties may be given. This also often implies additional oversight of the project
26	Lengthy FSR Development	A Feasibility Study Report (FSR) is a preliminary study undertaken to determine and document a project's viability. Because of the time it takes to carry out a feasibility study, business problems or legislative mandates are not quickly addressed. During a lengthy FSR process, requirements tend to change due to other influences and requirements
27	Lengthy RFP Development	A Request for Proposal (RFP) is an invitation for suppliers, through a bidding process, to submit a proposal on a specific commodity or service. A bidding process is one of the best methods for leveraging negotiating abilities and purchasing power with suppliers. However, the RFP process is lengthier than others are as the requirements are refined because of input back from vendors. Often this process requires more than one invitation to bid as well as interview with vendors before the final RFP is published. Delays are inherent in this process and place the project at a higher risk of schedule overruns.
28	MOTS (Modifiable Off-the-shelf) Software	Modifying COTS software is inherently problematic. There are many variables at play: what changes are required to conform the COTS to the business processes of the department, should any business processes be changed, do the modifications in the COTS affect its inherent performance, reliability, accuracy, etc. there are greater testing issues, and always the issue of post-implementation maintenance.
29	Not Adjusting the Schedule as Required	Failure to keep the schedule current almost always results in poor planning and poor execution. Although performing schedule updates can be a demanding and time-consuming task, it is critical to project success. Schedules are meaningless unless managed routinely, and kept up-to-date.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
30	Not Aligning Projects to Strategic Goals	When project does not align project objectives with the departmental strategic goals and business objectives, the project will be unlikely to receive the priority of attention from senior leadership and program staff. Clearly, approval authorities should scrutinize such a project very carefully before it goes forward.
31	Not Resource Loading the Schedule	Failure to resource load a schedule almost inevitably results in projects tasks not properly resourced and over-scheduling of key resources. The result is typically elongated schedules. Overuse of key staff fatigues them and may cause them to move on.
32	Politically Sensitive	Politically sensitive projects often receive increased scrutiny, which can distract the project team from its planned efforts. This environment also invites ever-changing requirements due to political influences.
33	Poor Change Control	It takes a strong change-control process to mitigate the impact of too many good ideas. The lack of change control and approval of new or changing functionality increases risks to project delays and cost overruns. In addition, the process may compromise users' expectations and acceptance.
34	Poor Change Management	Poor change management often means scope creep. In addition, users' expectations and acceptance may be compromised. One indication of the possibility of poor change management is lack of a project change management plan. A project change management plan is an excellent device to ensure all changes are properly vetted and that all stakeholders have a say in the outcome.
35	Poor Estimation Methods	Poor estimation methods can mean under-scheduling and under-budgeting. Projects normally do not identify poor estimation methods as a risk until schedules go awry or the project exceeds the budget. Poor estimates can affect schedule, resources, costs, and work effort.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
36	Poor IT Practices	This suggests that the department is not ready to manage projects on a degree of complexity. We identify this risk factor by the lack of documented Software Development Life Cycle, or IT processes and procedures. Without well documented and sound IT practices, projects are vulnerable at every stage of the process.
37	Poor System Integration	Poor system integration testing substantially increases the likelihood that the system will not functionally meet its intended use. Even more importantly, if the integration methods are substandard then often error and system performance degrades.
38	Poor Technical Support	Inadequate technical support for an IT system means users do not get their questions answered and problems addressed as needed and often results in users concluding that the system is a failure. User satisfaction is a major measurement of project success.
39	Poor Test Planning	A poorly tested system is a system likely to be deficient to some unknown degree. Nothing frustrates users and destroys the credibility of a system more than deploying it with many bugs. Another incentive for good test planning is the fact that the further down the project lifecycle system defects are identified, the more costly they are to fix.
40	Poor Vendor Competencies	Inadequate vendor staff can introduce into a project uninformed decisions, delayed decisions, and inappropriate outcomes at every step of the process, all of which can result in project failure. For example, skill shortages in vendor submission of resumes and references.
41	Poor Vendor Quality Management	Quality management is a broad issue including both outcomes and process. In other words, effective quality management is concerned with not only achieving appropriate outcomes, but also achieving them in an effective and efficient manner. Poor quality management is often detected by the absence of design walkthroughs, requirements validation, or quality assurance testing.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
42	Poor Vendor Risk Management	All projects incur risks, and the inability to manage successfully those risks results typically results in project failure. Poor risk management can result in schedule slippage, budget overruns, unsatisfactory quality of product, and failure to accomplish business goals.
43	Project Scope Too Large	Large and complex projects are particularly risky endeavors. Typically, they involve many players and extend over several years. Over time, multiple issues affect key staff changes, requirements change, and public sector budgets. When project scope is large, it increases the likelihood of project failure and makes the project much harder to manage.
44	Public Health and Safety	The team must exercise extreme quality assurance throughout the project, given that poor performance of the implemented software would adversely affect public health and safety.
45	Schedule Delays	Projects that experience schedule delays are at higher risk of project failure. Schedule delays not only elongate project schedules, but they also increase the likelihood of risks including higher costs, increased personnel turnover, and changing requirements.
46	Security	Projects where data security is an issue require an extra measure of expertise and approvals. The department must define appropriate security requirements up front and identify them in the project plan to mitigate the risk of security lapses. This includes data used for testing as well as post implementation.
47	Shortcut the Schedule	This activity is caused by incomplete data, or competing priorities within the department. Without proper data to support reducing project timeframes, there is the distinct possibility that the project can compromise deliverable quality. Alternatively, the project may have to eliminate functionality increasing the risk of unsatisfied users. For example, reducing project deliverable timeframes.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
48	Sole Source / Non-Competitive Bid	There is inherently no competition in this procurement scenario, leaving the organization with no alternative plan if the sole contractor cannot perform as expected. In addition, without competition, the cost is usually higher.
49	System Integration Consulting Services	This type of project typically involves more than one vendor. It is critical and difficult to keep all the players working together and committed to the same schedule. Departments procure system integration services for large, complex projects requiring varying skill sets. Increasing numbers of service providers involved increases the likelihood of risk.
50	Time and Materials	This risk factor identifies the use of a time and materials contract where the vendor provides services, but usually is not responsible for the development of a well-defined deliverable. The State should use this type of contract when the vendor is under the immediate supervision of a state IT professional, responsible for a portion of the project.
51	User Dissatisfaction	This factor identifies that the user is not satisfied by the project outcomes and believes one or more of the following: <ul style="list-style-type: none"> - The system does not meet business needs - The system is not user friendly - Key functionality is missing - Use requires changes to existing business processes
52	Vendor Underestimating Cost	There are many potential contributors to this problem. Often underestimating costs is symptomatic of other problems such as inadequate schedule management or budget management. In addition, if estimation techniques are poor and not all factors are considered, and then the project will likely be under budgeted, which is a recipe for failure.

ID	RISK FACTOR	RATIONALE FOR INCLUSION
53	Project Cost	This factor reflects the potential total loss to the state given a project failure and includes all one-time and continuing costs reflected in the approved Feasibility Study Report including any Special Project Reports.

Sample questions and answers to determine risk and impact

ID	RISK FACTOR	QUESTION	ANSWERS	IMPACT	MAX
2	COTS (Commercial Off-the-Shelf) Software	Does this project involve a COTS?	Yes No	9 0	9
3	Custom Development	Does the project involve custom development?	Yes No	9 0	9
4	Customer-in-Use	How long has the vendor's proposed solution been installed at time of bid submission?	< 6 months 6-8 months > 8 months	8 4 2	8
5	Data Center Support	Does the project involve Data Center Support?	Yes No	5 0	5
6	Lack of Vendor Experience with Multiple External Customers	How many years experience does the vendor have with multiple external customers?	Not Applicable Does Not Meet Meets Exceeds	0 9 5 2	9
7	Federal Funded/Penalties	Is this a federally funded project?	Yes No	5 0	5
8	Fully Outsourced New Development Services	Does the project involve fully outsourced new development services?	Yes No	9 0	9
16	Lack of Vendor Capability to Develop an Appropriate Project Plan	Is the Vendor's Project Plan Comprehensive and Feasible?	Not Applicable Not Feasible Acceptable Well Developed	0 8 4 1	8
18	Lack of Vendor Capability to Perform in a Cross Program Environment	How many years of experience does the vendor have with a multi-program project within a department (proven by references)?	Not Applicable Does Not Meet Meets Exceeds	0 9 5 2	9

ID	RISK FACTOR	QUESTION	ANSWERS	IMPACT	MAX
19	Lack of Vendor Capability to Perform in Multi-Agency Environment	How many years of experience does the vendor have with multiple agencies within a state project (proven by references)?	Not Applicable Does Not Meet Meets Exceeds	0 9 5 2	9
20	Lack of Vendor Capability to Perform in Multiple Local Governments or Counties Environment	How many years of experience does the vendor have with multiple counties and/or local governments within a state project (proven by references)?	Not Applicable Does Not Meet Meets Exceeds	0 9 5 2	9
21	Lack of Vendor Capability to Provide Appropriate Technical Architecture	Is the Vendor's proposed Technical Architecture not well-defined?	Yes No	0 5	5
22	Lack of Vendor Capability to Transfer Knowledge to State Staff	Has the vendor successfully transferred knowledge to the department staff in its previous projects (proven by references)?	Yes No	0 5	5
23	Lack of Vendor Management of Statewide Customers	Does the vendor lack statewide implementation experience?	Yes No	9 0	9
24	Lack of Vendor's PM Infrastructure or Methodology	Does the vendor lack a Project Management infrastructure or methodology?	Yes No	8 0	8
25	Legislative Mandate	Does the project involve a Legislative Mandate?	Yes No	8 0	8
27	Lengthy RFP Development	How long is the RFP development?	Not Applicable < 6 months 6-12 months > 12 months	0 1 5 7	7
28	MOTS (Modifiable Off-the-shelf) Software	What is the percentage of modifications required?	Not Applicable < 10% 10-30% > 30%	0 2 5 8	8
32	Politically Sensitive	How political is the project?	Not Political Somewhat Political Extremely Political	0 5 9	9
44	Public Health and Safety	Does the project affect public health and safety?	Yes No	7 0	7

ID	RISK FACTOR	QUESTION	ANSWERS	IMPACT	MAX
48	Sole Source / Non-Competitive Bid	Does the project involve a Non-Competitive Bid?	Yes No	5 0	5
49	System Integration Consulting Services	Does this project involve Systems Integration Services?	Yes No	9 0	9
50	Time and Materials	Does the project include a time and materials contract?	Yes No	7 0	7
52	Vendor Underestimating Cost	Did the vendor underestimate the cost?	Yes No	5 0	5
53	Cost (separately discussed)	What is the total cost of the project?	< \$10M \$10-50M \$51-\$100M > \$100M	4 6 8 9	9