Procurement: Avoiding Risky Business

NASCIO IT Procurement Modernization Series: Part III

September 2013

NASCIO Staff Contact:
Meredith Ward
Senior Policy Analyst
NASCIO

NASCIO represents state chief information officers and information technology executives and managers from state governments across the United States. For more information visit www.nascio.org.

201 East Main Street, Suite 1405
Lexington, KY 40507
Phone: (859) 514-9153
Fax: (859) 514-9166
NASCIO@AMRms.com
www.NASCIO.org

In the 2012 State CIO Survey: Advancing the C4 Agenda, 46% of state chief information officers (CIOs) expressed some form of dissatisfaction with the current form of IT procurement in their states. As one CIO stated, "purchasing IT equipment and services is treated the same as buying paper products, with no consideration for the complexities and subtleties of IT systems." This sentiment is not new. Previous surveys of the state CIO community reveal similar findings and frustrations with both the process and outcomes.

Taking these frustrations to heart, NASCIO has sought ways to encourage collaboration between CIOs, chief procurement officials and private information technology (IT) sector vendors. The NASCIO IT Procurement Modernization Committee, in partnership with TechAmerica[i] and NASPO[ii], continues to focus on state IT procurement reforms and highlighting best practices at the state level. This brief is the third in a series of recommendations set forth by this collaborative.

The purpose of this brief is to highlight some of the strategies used to first identify, then to avoid, transfer, mitigate, and ultimately accept the risks associated with the procurement of IT products or services. Although not all risks can be identified, the goal should be to understand how much risk is associated with a specific IT procurement and what tools, processes, benchmarks, and methodologies are available to uniquely address IT procurement risks.

INFORMATION TECHNOLOGY: WHY RISK IS DIFFERENT

Management of risk is one of the greatest challenges facing IT procurement and service delivery today—the goal of which is to ensure successful procurement of technologies with a secure supplier, under terms that the entity is able to adhere to, that enables flexibility to withstand the potential challenges of the subsequent supplier/source relationship.

IT procurement-related risk is highly situational and the nature and degree of risk may vary quite considerably for each procurement. IT procurement risks can source from the creation of a Request for Proposal (RFP) that embodies novel technology, or from the inability to fully articulate the requirements. Internal agency process and procedures, governance, stakeholder work, contract terms and conditions, or implementation and payment structure can also present IT procurement-related risk. These risks can be financially significant. As an example, a contract for a moderately complex application will require expertise in procurement, application complexity estimation, networking, security, legal, business process subject matter experts, and potentially other discipline-specific expertise. If procurements go awry, the cost of resolving them can quickly amount to millions of dollars.

IDENTIFYING RISKS

In order to know how to address risk, risk possibilities must be assessed from many perspectives. The hallmark of any great team is their ability to collaborate, and to best identify risks, a very diverse team is needed.

Potential risks should be listed and the list streamlined to ensure the risk statements are clear and not duplicative. The team should assess the likelihood that the risk will occur and the potential severity of the impact. One example of a risk matrix appears in Figure 1 below. The risk assessment team would place each identified risk along the probability and impact scale to determine the need of developing a specific risk strategy for those discrete risks deemed likely and of great impact.

Example Risk Matrix ***Figure 1***

Likelihood of Event Occurrence	Event Severity **Extreme** Level X Event	**Major** Level 3 Event	**Moderate** Level 2 Event	**Minor** Level 1 Event
Remote	• Targeted Terrorism • Loss of Life (workplace violence)	• Major Supply Chain Disruption • Major Natural Event (Hurricane, Tornado, Earthquake) • Internal Sabotage • Cyber Terrorism	• Minor Supply Chain Disruption	• Impacts on Normal Operations • Failure to document all requirements at the beginning of the procurement/ project
Low Probability	• Severe Brand Damage • Political Instability • Level 1 Terrorism • Loss of Key Sponsors	• Transportation Infrastructure Disruption • Telecom Infrastructure Disruption	• Kidnap & Ransom • Facility Fire • Major Flooding • Minor Natural Event	• Feature creep (incorporation of additional features during the project) • Failure to understand and document business processes related to the procurement
High Probability	• Major Hazmat Incident	• Worksite Accident • Loss of Life (limited) • Delays associated with subcontractors or third-party stakeholders	• Attrition of Key Personnel • Knowledge Capital Loss • Telecom Outage	• Attrition of Non-Essential Personnel
Anticipated	• Major Natural Event (Hurricane, Tornado, Earthquake) • Epidemic		• Power Outages	• Minor Flooding

One source of risk often overlooked is the risk associated with the application size. For instance, according to Capers Jones, a specialist in software engineering methodologies with Namcook Analytics and an expert witness in 12 lawsuits for projects that either failed or did not work as promised when delivered, software application size can be measured by function point. A

function point is a unit of measurement to express the amount of business functionality an information system provides to a user.

The main purpose of sizing an application is to understand the degree of risk faced relative to other IT projects. Thus, an ERP implementation is often the most risky project undertaken by an organization. For state government, complex and multifaceted systems procured to support federal programs are also in this category.

With that ground work laid, the project team is ready to start planning how to address risk. At a high level, risk can be addressed through one of four ways: **avoidance; transfer; mitigation; and acceptance**.

RISK AVOIDANCE

Risk avoidance is where threats are identified and categorized -- and avoidance options are measured and strengthened to detect, prevent and react to an event trigger.

Strategies employed in risk avoidance efforts by states include:

- Prior to issuing an RFP, use a formal interview process for direct contact with IT staff from other states that procured and implemented a similar solution. The NASCIO Community is an excellent resource to identity states with experience in projects under consideration. The lessons learned can be invaluable;
- Alignment with the state's enterprise architecture (see NASCIO's Leveraging Enterprise Architecture for Improved IT Procurement);
- Policies and standards that require the use of interoperable technologies;
- Construction of contracts with clear deliverables (itemizing milestones and payments upon completion and holdbacks of final payment upon written acceptance);
- Contractual requirements which prohibit the use of smaller vendors in critical governmental infrastructures;
- Independent validation and verification of work as work is performed (generally constructed as an independent vendor regularly reviewing and reporting on the activities of the primary vendor to ensure the needs of

the client agency are met and the system complies with the requirements and specifications); and

- Effective software defect removal procedures and practices.

Oregon recently negotiated an e-government portal replacement contract which faced a number of severe risks. One of the risks was that the new portal provider would not be up and running before the contract with the old portal provider expired. Oregon was faced with two severe transition risks:

1. Not having an operational portal delivered on time - this risk was deemed unacceptable and had to be avoided.
2. The necessity to pay the old contractor to continue operating the old portal and while also paying the new portal provider.

The schedule was tight so there was a high likelihood that one of these scenarios would be realized. The project team developed a tactic that allowed for an additional negotiated extension with the old contract to keep the portal operational. There was a provision in the new contract requiring the new contractor to pay the state for the cost of any extension as a result of any delay related to their performance that would require the previous contract to be extended.

While the transition was difficult, Oregon avoided a complete business disruption by transferring this risk through the contract with the new contractor. Oregon was very fortunate that the existing contractor and the new contractors worked with the state as strategic partners during this transition.

IBM discovered many years ago that projects topping 95% in defect removal efficiency had shorter schedules and lower costs than those below 85%. This is because the effort to find and fix defects is greater late in the development cycle than it is early in the development cycle. Therefore successful large software projects are very proactive with design and code inspections, since only formal inspections plus formal testing can top 95% in overall defect removal efficiency.

One sign that a vendor is likely capable of handling large applications development is if they utilize state of the art quality control methods. The state of the art for large software applications includes sophisticated defect prediction methods,

measurements of defect removal efficiency, utilization of defect prevention methods, utilization of formal design and code inspections, presence of a Software Quality Assurance (SQA) department, use of testing specialists, and usage of a variety of quality-related tools such as defect tracking tools, complexity analysis tools, debugging tools, and test library control tools.

In performing post-mortems of cancelled or failed projects, it is fairly easy to isolate the attributes that distinguish disasters from successes. Experienced project managers know that false optimism in estimates, failure to plan for changing requirements, and inadequate quality approaches lead to failures and disasters. Conversely, accurate estimates, careful change control, and top-notch quality control are stepping stones to success.

RISK TRANSFER

Risk transfer is primarily focused on providing financial protection against the quantitative impacts of an event. Historically, one approach to this has been in the form of an insurance instrument designed to reduce the level of financial risk associated with the procurement.

As discussed in NASCIO's publication, Gaining Traction on the Road to Win-Win: Limitations on Liability in State IT Contracting, NASCIO supports providing vendors, partners and suppliers with clear and reasonable liability provisions. It is in the best interest of the state to not constrain the market place and allow a competitive bidding process. Companies have recognized the risk and vulnerability of placing an entire business in jeopardy for a contract that is minimal in comparison to the total value of its assets. Because of unlimited liability for vendors in several states, some choose not to participate.

But in an effort to level the playing field between large and small vendors there has been an increase in the number of requests for limitations of liability clauses written into the procurement contracts. In most instances the state IT contracts have resulted in one of the following policy approaches: the state has boilerplate language that it uses when assessing risk-management, the state may adhere to a set of terms for limitations of liability on a case-by-case basis, the state may require costly insurance, the state may require the purchase of a performance bond, or the vendor may decide to not pursue

the contract after the state declined to offer limitations of liability. States have claimed that unlimited liability rules or policies narrow the scope of competition in the marketplace.

Risk transfer (or shifting) approaches should be clearly understood by both the contractor and the state. Contract terms and conditions must be carefully negotiated between the state and the provider so that risks are clearly articulated and the contract reflects clear intent to transfer. Any risk shifting has tradeoffs and cost considerations, and risks under the direct control of the state cannot be legally transferred to the contractor.

Strategies employed in risk transfer efforts by states include:

- Negotiating liability terms and conditions;
- Insurance policies;
- Using cooperative procurement vehicles, such as the WSCA-NASPO Purchasing Organization and, for eligible states, the GSA Schedule 70;
- Performance bonds;
- Collaboration with states who may provide needed services; and
- Other financial instruments.

Often the instrument itself fails to provide the transfer of risk hoped for (see Leaving Performance Bonds at the Door for Improved IT Procurement).

Additionally, this transfer of risk does nothing to address qualitative impacts—for example damage to relationships or damage to image—which often accompany large-scale procurement failures and represent the most significant long term effects.

One way to address IT project risks is to thoroughly address them upfront during the procurement process and before the contract is signed, instead of the more traditional approach which leaves critical project items to post contract signing. IT attorney Dennis Gallitano has developed a multi-staged procurement process which includes full project planning, and addresses the more common risk issues as part of the contract negotiations.

As reflected in Figure 3, the traditional life cycle of a procurement starts with the identification of need, evaluation of options, the issuance of an RFP, selection of a "vendor of choice" (or apparent successful vendor), followed by the negotiation and signing of a contract. Project planning and preparation typically is limited to reviewing sample statement of work and project plan templates, as opposed to project documents that are tailored to the specific needs of the customer or project. After the contract is signed, there is a project kick-off where the important project documents are reviewed.

Typical Lifecycle ***Figure 3***

The main drawback to the traditional procurement approach is that the customer has lost its procurement leverage to ensure that important project documents are developed with the types of commitments needed to make the project successful. In Gallitano's staged approach, the project planning is sequenced into the procurement process upfront to ensure that all key project requirements are met and the vendor commits, in writing, to these requirements. Figure 4 below depicts where project planning can be sequenced.

Revised Lifecycle ***Figure 4***

Project planning, which Gallitano refers to as Implementation Planning Study, includes a series of workshops to develop a detailed statement of work, a detailed project plan that includes the agreed to phasing and deployment strategies, a month-by-month, by service category, joint resource plan, a project management plan, a quality assurance plan, and other project documents and tools (such as the issue management plan and risk management plan). As part of the procurement

process, Gallitano recommends developing these templates ahead of time so they can be made part of the RFP. In that way the vendors bidding on the project will be required to react to the customer-prepared project documents, instead of the customer having to react to vendor-prepared documents.

RISK MITIGATION

Risk mitigation is how to respond to and recover from a disruptive event, thereby reducing the negative consequences should the event occur. Mitigation can come through identifying likely outcomes and codifying policies or procedures to detect, notify, and mitigate the negative consequences of problems. Historically, mitigation has reduced the number and size of interruption claims.

Strategies employed in risk mitigation efforts by states include:

- Contractual constructs in the form of defining arbitration processes;
- Definitions of functionality required;
- Defining the process and expected costs to accommodate requirements changes;
- Developing strategic partnerships to incentivize the best performance out of both partners;
- Service level agreements; and
- Associated penalties for performance failures.

Capers Jones suggests that, for software development contracts, an effective way of dealing with changing user requirements is to include a sliding scale of costs in the contract itself. For example, suppose a hypothetical contract is based on an initial agreement of $1,000 per function point to develop an application of 1,000 function point in size, so that the total value of the agreement is $1,000,000.

The contract might contain the following kind of escalating cost scale for new requirements added downstream:

Initial 1000 function points
= $1000 per function point

Features added more than 3 months after contract signing

= $1100 per function point

Features added more than 6 months after contract signing
= $1250 per function point

Features added more than 9 months after contract signing
= $1500 per function point

Features added more than 12 months after contract signing
= $1750 per function point

Features deleted or delayed at user request
= $250 per function point

RISK ACCEPTANCE

Risk acceptance is when there is a clear understanding of and confidence in the vendor and staff's ability to respond to a disruptive event or delivery failure. This is only possible with the successful execution of risk identification, avoidance, transfer, and mitigation strategies previously discussed. Risk acceptance has three tiers:

1. Acceptance levels for hardware;
2. Acceptance for software; and
3. Acceptance for services (services may even be decomposed to two or three levels as well: services which are commodity in nature [a java programmer, a desktop computer support person] and those which are professional services in nature [management consulting]).

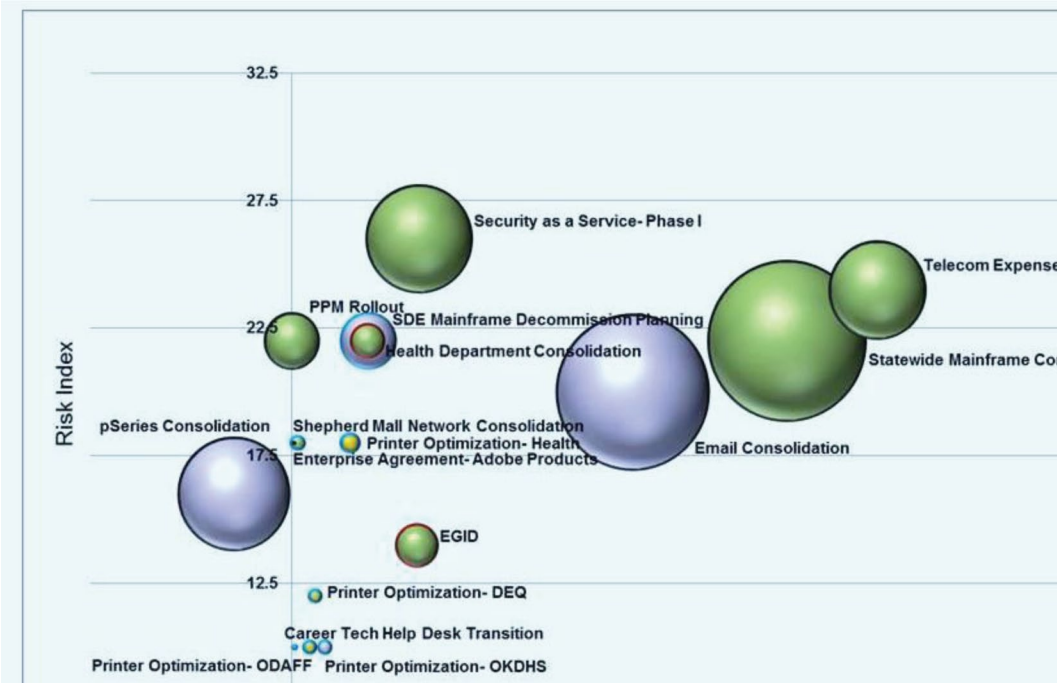
From an IT procurement perspective, risk acceptance can only occur after the team has fully understood, appreciated and assessed each of the risks presented. Once strategies are developed to avoid, transfer, and mitigate, the focus must shift to the decision process to determine the level of acceptability. Often in IT projects, business executives are not briefed on the risks and participate in the actual go/no go decisions of the technology investment. Walking through the scenarios with business leadership and allowing them to help shape the decision not only provides acceptance, but also provides buy-in, support, and understanding.

One example of illustrating and gaining acceptance is Oklahoma's "beach ball" chart (Figure 5), depicting the IT consolidation portfolio in the form of colored balls. The size of the ball indicates the investment required, which is defined

as the first year cost of the project. The vertical axis (Y) represents a measurement of project risk). A standard approach to identifying and quantifying key attributes of project risk is used to create a risk index to compare relative risk across different projects.

Some of the project attributes that are quantified include the number of agencies involved in the project, the technical and business complexity, the number of function points the software provides, the length of the project and the estimated accuracy of the project estimates. This then becomes a forced ranking of estimated impact to the state should something go wrong. The horizontal axis represents the Net Present Value (NPV) for the project. Only projects with a positive NPV based upon cost reduction are recommended to be undertaken, with the savings going back to the agency after the cost of transformation has been paid. Using this process, the IT governing board reviews the risk in context of the estimated return to the state for each project and decides if it is worth pursuing.

Figure 5



Source: Alex Pettit, CIO, State of Oklahoma

WHAT's NEXT

During their tenure as state CIOs, all will have some involvement in major IT procurements and all will be faced with helping to determine the appropriate amount of risk to accept.

Risk management in state government requires consistent diligence even after the initial approach is determined, as IT procurement-related risks can evolve and change during the project and necessitate additional contracting activities to support successful project completion.

Some questions for states to consider are:

- What stakeholders in your state are involved with identifying risk for IT procurements?
- What strategies has your state used for risk mitigation?
- Has your state developed policy in regards to risk acceptance on IT projects?
- Are there processes in place to mediate any business failures?
- Is your state using metrics to track progress on state IT projects?
- Are project managers prepared for change control and project revisions?

However, it should be noted that even when all of the information in this brief is put to practice, the greatest way to minimize risk is good governance, shared expectations and realistic goals from the start. It is critical that CIOs keep the conversations going in their own states and continue to collaborate with their state procurement officials and the private sector to ensure the best possible outcomes for all involved.

As Col. Green in the movie, The Bridge Over the River Kwai said, "even when it's finished, there's always one more thing to do."

---

[i] TechAmerica is the leading voice for the U.S. technology industry – the driving force behind productivity growth and job creation in the United States and the foundation of the global innovation economy. Representing premiere technology companies of all sizes, we are the industry's only trade association dedicated to advocating for the ICT sector before decision makers at the state, federal and international levels of government. With offices in Washington, D.C., Silicon Valley, Brussels and Beijing, as well as regional offices around the U.S., we deliver our members top tier business intelligence and networking opportunities on a global scale. We are committed to expanding market opportunities and driving the competitiveness of the U.S. technology industry around the world.

[ii] NASPO is a non-profit association dedicated to strengthening the procurement community through education, research, and communication. It is made up of the directors of the central purchasing offices in each of the 50 states, the District of Columbia and the territories of the United States. NASPO is an organization through which the member purchasing officials provide leadership in professional public procurement, improve the quality of procurement, exchange information and cooperate to attain greater efficiency, economy, and customer satisfaction.

Contributors and Reviewers

Alex Pettit
Chief Information Officer, State of Oklahoma

Dugan Petty
Immediate Past President, NASCIO

Dennis Gallitano
Special Assistant Attorney General, State of Washington

Capers Jones
Namcook Analytics

Carol Henton
Vice President, State & Local Government, TechAmerica

Jack Gallt
Executive Director, NASPO

Rebekah O'Hara
Consolidated Technology Services, Chief Legal Services Officer, State of Washington

Chad Grant
Senior Policy Analyst, NASCIO

Kristen Judge
Executive Director, Trusted Purchasing Alliance, Center for Internet Security