Strategic Risk for Government Procurement Attorneys

NASPO LEGAL EDUCATION™

Government procurement has never been more dynamic or full of opportunity. As cloud technologies are embraced along with AI-powered services, attorneys on both sides of the contracting process are navigating an exciting but complex landscape. This new era of technological integration comes with new and often unknown risks, making the issue-spotting and mitigation attorneys do even more difficult.

It is commonly said among attorneys that there's a reason we call it "risk management or mitigation" and not "risk elimination" – because everyone can accept that risk cannot ever be eliminated in any circumstance, let alone in the complicated world of public procurement. What is left for us to decide is how we deal with the risks presented during the government contracting process, and that is where the opportunities to practice strategic risk emerge.

When it comes to risk, strategic thinking can make the difference between mediocre outcomes and lasting success. Today's procurement and contracting attorneys – whether representing governments or suppliers – have unique opportunities to craft agreements that deliver genuine value while managing evolving risks in cybersecurity, data government, and digital accessibility.

Government attorneys can seek to maximize value for taxpayers, and supplier attorneys can work to build sustainable government partnerships by understanding shared challenges and collaborative solutions. The hope is that we can move beyond traditional adversarial negotiations to develop contracts that will truly serve the public interest while supporting innovative solutions.

In this paper, we will:

- Explain what a strategic risk management approach is, and how to apply it to government contracting;
- Provide understanding on the government's view of risk;
- Share the benefits of contracting with the government for suppliers; and
- Discuss what proper strategic risk management looks like in practice with tools for implementation.

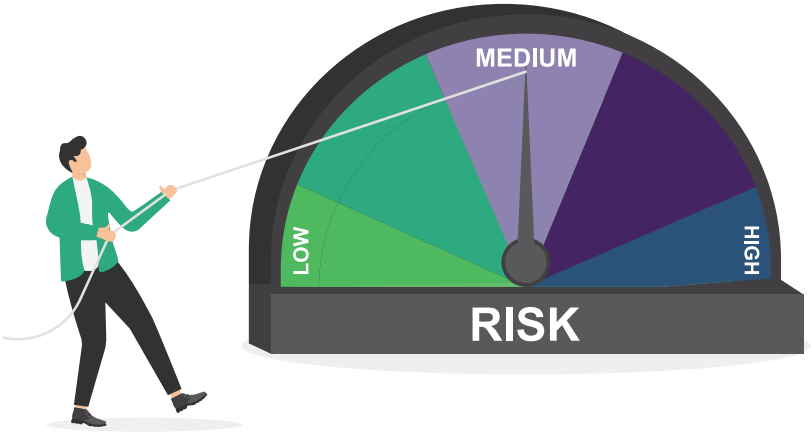
What is "strategic risk?"

An experienced rock climber would never gear up, walk up to an unknown granite wall, and simply start climbing, assuming they will figure the route out on the way up. This would be not only be dangerous, but most likely unsuccessful. Instead, the successful climber would scout the route before attempting a big climb, talking to fellow climbers and researching the location, determining the best conditions in which to climb, preparing the appropriate equipment they will need based on all of the information they gathered, and showing up prepared with a plan and a route they have vetted and/or practiced beforehand. This scenario exemplifies "strategic risk" – yes, it is risky to climb a mountain face, but one can significantly reduce the amount of risk through preparation and planning.

A commonly overlooked strategic risk is the exposure of the fallacy of believing the status quo is good enough - in other words, it can be riskier to not act in some situations. **This reality leads to the acceptance of some risk as long as it has been considered, discussed, and planned for.** For example, not updating large software systems and having them fail, lose data, or become easily breached is far more difficult to manage than a planned upgrade that may have some bugs, but ultimately will result in improved systems with better security.

How does the government define risk?

Government procurement involves the spending of taxpayer dollars and therefore carries the responsibility to ensure the money is spent wisely and in the best interests of the citizens. This is an essential truth that drives most of the law and policy found on public procurement.



Risks to the taxpayer dollar being spent unwisely include, but are not limited to:

- Conflicts of interest
- Vendor bid-rigging or other collusion
- Difficult technology integration due to legacy systems
- Decades-old infrastructure
- A procurement cycle that doesn't match the modern technology lifecycle
- Price-fixing and/or gouging
- Obstacles to meaningful supplier oversight
- Decreasing staff sizes in government agencies to deal with all of these risks

Why is the government so adverse to risk?

The "hallmark" terms of public procurement mark the key elements to ensuring that public tax money is spent appropriately: **fair, open, and transparent competition among qualified suppliers for government contracts.**

Each state's citizens are required by law to interact with the state on some level. If a private company has a large data breach, a consumer can just switch to another company – not so with the government. A unique duty exists for the government to protect the data of its citizens.

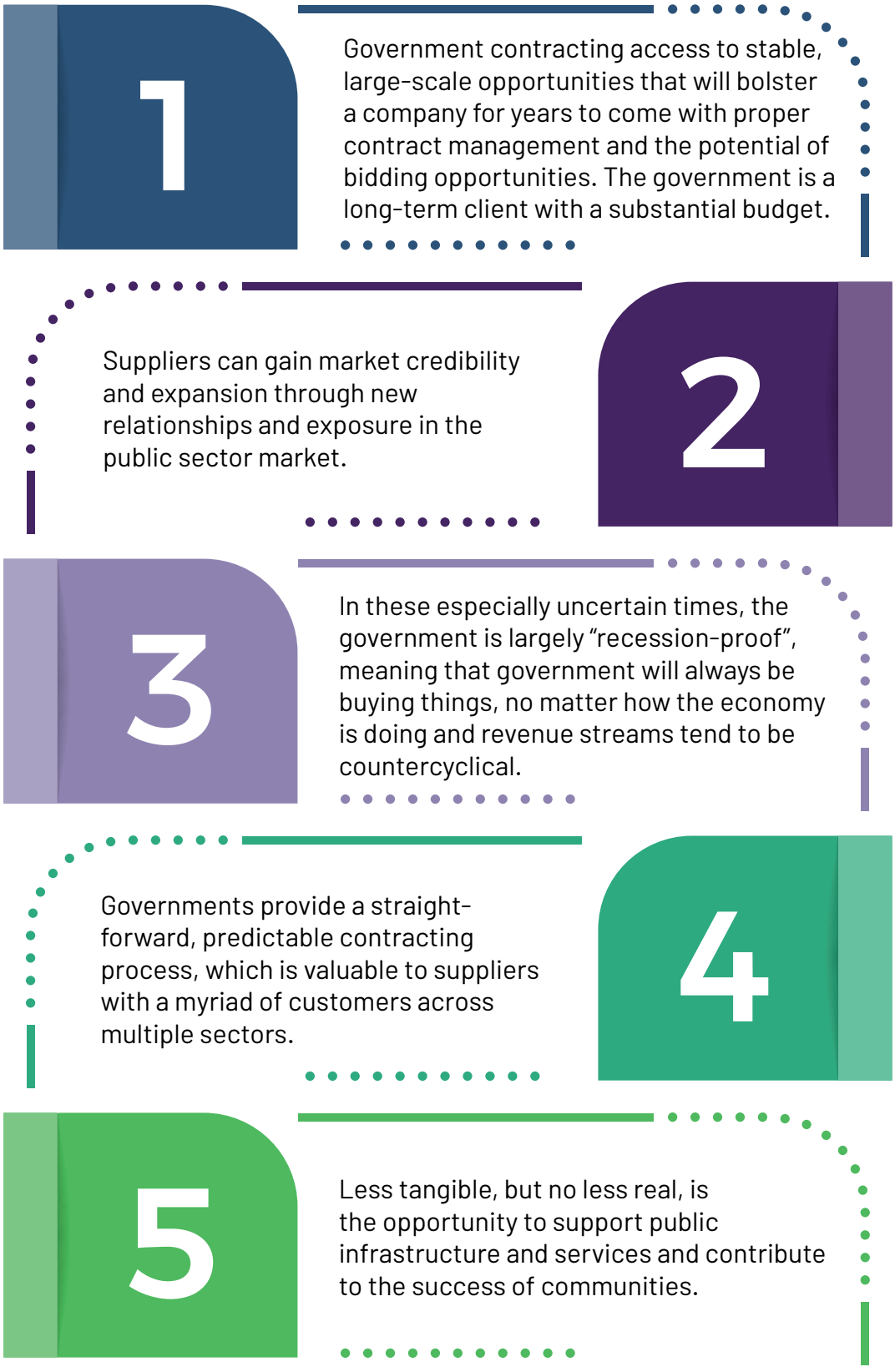
Why is it important to be so sensitive to risk when the interconnectedness of our technology has led to the unfortunate truth that data breaches are commonplace? The protection of sensitive data is not merely a best practice but a legal mandate, evidenced by heightened procurement standards following high-profile breaches of citizen information. The public servants who work on government procurement believe they must hold this trust of information sacred.

Further complicating matters are constitutional and statutory limitations on liability that shape how states structure contracts and partnerships, often requiring extensive indemnification clauses. Ultimately, risk-averse procurement stems from the non-negotiable reality that government functions must continue without interruption—citizens depend on consistent service delivery regardless of technological or supplier challenges, making the stakes for procurement decisions exceptionally high.

What are the benefits to suppliers when they contract with the government?

It may seem daunting to take on the responsibilities of a government supplier, but the benefits may entice a company to be strategic about the risk they assume and work with the government to get to mutually beneficial contract terms. For government attorneys, it is important to be able to speak to the positive aspects of working with government since so much time is typically spent discussing the downsides.

Benefits to consider and share include:



All that being said, a company should still take a hard look at whether government contracting is right for them – weighing the risks and then making a determination based on the facts you have is what turns risk into "strategic risk!"

Proper Strategic Risk Management and Assessment

There is not a one-size-fits-all approach to strategic risk management and it is important to properly assess any risk before venturing too far into the woods on any procurement project. What does proper risk assessment involve?

- An attorney is a legal subject matter expert (SME) for the procurement team. Legal counsel should be involved early and often in the process of any procurement. Knowing the potential pitfalls of a procurement from the start can lead to smoother approval processes when it comes time to sign the contract.
- Attorneys can assist the procurement team in understanding the law and policy that applies to the procurement in question.
- Use non-legal SMEs as appropriate to counsel and advise on the best way to procure the good or service in question.
- Legal can rely on research provided by the procurement team, but should ensure they understand the implications of the compiled data.
- Use other legal resources and contacts!
- Utilize continuing legal education opportunities and resources to increase general knowledge of the newest risks in public procurement.

Common Risks in Modern Procurements

The procurement of technology services and equipment is the most common place we can easily identify risk in modern government procurement – but there are many other sources we should consider. In this section we will explore those major risks and discuss how to avoid these common pitfalls.

The following list of potential risks is in no way meant to be exhaustive. Please check with your own government's requirements, laws, and policies.

Budget Overruns and Cost Escalation – Projects frequently exceed initial cost estimates due to scope changes, unforeseen challenges, and/or inadequate planning. These types of budget issues can lead to concerns about appropriations and violations of the law. These risks are difficult to plan for, but knowledge is power and it is important to equip oneself with the laws and policies of your state as a cloak against the winds of uncertainty.

Specification Challenges – If the specifications for a procurement are not well defined and the problem the end-user is trying to solve is not well articulated, a procurement can fail once significant energy has already been dedicated. Ensure that specifications are written with fair competition in mind, allow for creative solutions from the supplier community, and include the supplier community in Q&As and RFIs prior to issuing a bid to ensure that specs comply with current industry standards.

Data Privacy Vulnerabilities – Systems that require vast amounts of sensitive Personal Identifiable Information (PII) should be considered a data exposure risk and require meticulous compliance with privacy regulations. Be aware that it is not only software systems that may expose the state to a breach, and consult the experts.

Intellectual Property and Supplier Dependency – Governments must ensure that any proprietary solutions of any type should allow licensing to the government of the intellectual property usage, right to repair, and/or insufficient transfer of skills and knowledge from the supplier to government staff for future maintenance and operation. These obligations should be in the contract and understood clearly by all parties before any work is begun.

IT Specific Risks – There are some risks that come inherent in any procurement that involves technology, especially software. A good rule of thumb: if it is connected to the internet AND is a government-owned device, there can be a breach. Other unique risks to look out for in IT contracting include, but are not limited to:

Algorithmic Bias and Fairness Concerns – Artificial intelligence systems may perpetuate or amplify existing biases in historical data, potentially leading to discriminatory outcomes in public services.

Lack of Transparency – Many IT companies consider themselves "black boxes" of proprietary information and therefore lack transparency in their reasoning processes. This can conflict with the government's duty to be open with the citizens.

Rapid Technological Obsolescence – Technology evolves rapidly, potentially rendering significant investments in large-scale projects essentially outdated before the procurement cycle is even completed. Additional procurement methodologies, such as agile procurement, can be explored to mitigate this risk.

Liability Allocation – The determination of fault and liability when it comes to technology and use by the government is largely unsettled. We can look to caselaw and settled precedent for the issues often raised by non-IT procurement liabilities – but not so with, for example, large-scale software systems implementation. Ensure that contractual terms are crystal clear to all parties and use the Statements of Work and other planning documentation to allocate responsibility fairly and appropriately with consequences outlined. It is rare that indemnity clauses become the subject of litigation between the government and a supplier, so don't allow that to be a crutch for avoiding good contract practices.

Supplier Performance Issues – The days of accepting the lowest price bid without further criteria have long passed us by. Procurement offices can now be sophisticated arbiters of the fitness of a supplier for a particular project by using market research tools and databases such as GovWinIQ and ProcurementIQ.[1] Even so, supplier performance issues can emerge. Managing this risk involves meticulous contract management systems and tools alongside an educated and empowered procurement team holding suppliers accountable.

Outside Pressures – Beyond the procurement process itself, organizational challenges, workforce issues, loss of institutional knowledge, politics, and unrealistic expectations on the procurement team can lead to a myriad of additional risks. These are, unfortunately, something every government procurement professional will deal with at some point in their career and it is important to seek support and help from your colleagues and legal staff.

These are the generalized risks for most public procurements – there is a more specific checklist for strategic risk planning at the end of this paper. Please use that as a framework to develop your own checklist that incorporates all of your jurisdictionally-specific requirements.

[1] If you are a NASPO member, reach out for access to GovWinIQ and ProcurementIQ: info@naspo.org

Negotiating for Success on Risk

Being successful in negotiating around potential risks is truly about making the best decision you can with all of the information you have at a given moment in time. Here are our top tips to take into your next negotiation:

1. Gather all of the information available to you. Know your facts and you'll be able to speak intelligently to any issues that arise during the negotiation. Utilize SMEs where you can and bring in the end-users to determine true needs.

2. For suppliers, understanding the government's position on liability before you get to the negotiation table can save a lot of time and effort. Consider developing a set of "government-friendly" terms and conditions based on your own research on the requirements and laws of the jurisdiction with which you are contracting.

3. Look for opportunities to discuss a particular procurement's contract terms and conditions, especially if they differ from standard Ts and Cs, such as Q&A sessions with the supplier community and the use of RFIs and RFQs.

4. Ambiguity is not your friend. Do not agree to terms you are uncertain of and/or rely on the idea that you can argue your point later. Maintain an open line of communication during redlining to allow explanation of additions and deletions for the clarity of all.

5. Utilize innovative procurement methodologies such as agile or iterative procurement, robust and well-defined Statements of Work, and other contractual mechanisms for mitigating and isolating risk where you are able.

Conclusion

As we all know, risk cannot be eliminated — it must be managed intentionally and with dedication that recognizes the importance of avoiding risk in the public interest. A strategic approach to risk recognizes that risk avoidance should not prevent necessary modernization or perpetuate failing systems. You can make turn the risk of climbing an unknown rock face into a strategic risk with a higher chance of success by planning for and contracting smart solutions to risk management. Large and complicated procurements can be made manageable, and you can reach the top of the mountain!

Additional Resources:

1. Attorney Roundtable Paper

2. Legal Research Toolkit

Strategic Risk Assessment Checklist for Government Contracting Attorneys

Pre-Procurement Risk Assessment

Public and Political Impact

- ☐ Could the failure of this system or service affect public safety or essential government functions?
- ☐ Would problems with this contract likely generate media attention, administrative, or legislative scrutiny?
- ☐ Does this procurement involve politically sensitive data or populations?
- ☐ Are there any upcoming political transitions that could affect contract continuity?
- ☐ Would contract failure require emergency appropriations, regulatory, or legislative action?

Financial Exposure Analysis

- ☐ What is the total potential financial exposure? This may include contract value, the potential damages, and/or replacement costs.
- ☐ Are there auto-renewal clauses? What are the terms?
- ☐ Does the pricing model create budget unpredictability on the government or the supplier?
- ☐ What would be the true cost of early termination for any reason?
- ☐ Are there "hidden" costs for implementation or integration?

Technology and Data Risks

- ☐ Will the supplier have access to Personally Identifiable Information (PII), public health information, or other sensitive government data?
- ☐ Are there data residency or sovereignty requirements to consider?
- ☐ Does the system integrate with the current critical government infrastructure?
- ☐ Are there cybersecurity standards the supplier should meet? (NIST, FedRAMP, state-specific?)
- ☐ Will the system be making any automated decisions that affect either citizen rights or benefits? If so, what mitigation is there for bias or discrimination?
- ☐ Does this contract invoke requirements of compliance with the ADA digital accessibility requirements?

Contract Terms Review

Performance and Accountability

- ☐ Are performance standards measurable, understood by all parties, and enforceable by the government?
- ☐ Do service-level agreements actually compensate for realistic damages?
- ☐ Is there a termination-for-convenience clause? If so, what are the implications for the supplier if the government chooses to exercise this right?
- ☐ Are there any liability caps? Are they reasonable given the potential government damages?
- ☐ Will the supplier accept responsibility for data breaches that involve state data? What will that look like?
- ☐ Is the government creating a risk of supplier dependency that may not allow for reasonable transition to another supplier if necessary?
- ☐ What are the data export/portability rights?
- ☐ Does this contract use proprietary terms or formats that may create issues with intellectual property?
- ☐ Are there source code escrows required for critical custom systems?
- ☐ If the contract is terminated for any reason, will there be any transition assistance?

Legal Compliance Gaps

- ☐ Do the contract terms comply with all relevant laws and constitutional requirements?
- ☐ Are public records and transparency obligations of the government considered?
- ☐ What are the audit rights and compliance monitoring provisions?
- ☐ Is there a force majeure clause and does it protect everyone's interests in the event of an emergency?

Supplier Stability (The government should consider these points, and the supplier community should prepare answers when negotiating with government to these key concerns.)

- ☐ What has been the supplier's financial status over the past three years?
- ☐ Is there any pending litigation, bankruptcy filings, or regulatory actions involving the supplier?
- ☐ Does the supplier's insurance coverage meet contract requirements?
- ☐ Does the supplier have an overdependence on key clients (aka customer concentration risk)?
- ☐ Can the supplier handle the scope and scale of the government requirements?
- ☐ Are there any reviews/references from other government clients of the supplier?
- ☐ What plans does the supplier have in place for business continuity and/or disaster recovery?
- ☐ What are the key personnel from the supplier involved in the contract and what happens if those personnel leave supplier's employ?
- ☐ What are the supplier's security audit procedures and certifications?
- ☐ Does the supplier comply with relevant industry standards and practices?
- ☐ What oversight is being provided for any subcontractors?

Implementation Risk Controls

- ☐ Ensure there is a clear project governance structure with government oversight.
- ☐ What are escalation procedures for problems and disputes?
- ☐ When will reporting be necessary and will there be milestone reviews?
- ☐ Is there a method for scope change and approval?
- ☐ What are the cost controls for modifications and additions?
- ☐ What is a significant change that may lead to the need for an impact assessment?
- ☐ Ensure that all changes to any agreement are in writing and reviewed by all legal parties involved.
- ☐ What are the key metrics for the supplier to meet? Are there regular performance review meetings?

- ☐ Is there a method for documenting performance issues and supplier responses?
- ☐ How will supplier personnel changes and knowledge transfer work?
- ☐ Consider notification requirements for internal stakeholders of both the government and supplier when key changes are made.

Quick Decision Framework

Your contract may be high risk if you answer YES to any of the following:

- Contract failure would affect public safety or essential services
- Total exposure (financial, reputational, and operational) is significant
- The supplier will have access to sensitive data and/or makes automated decisions
- There are limited alternatives if the supplier relationship fails
- Political or media attention is likely if problems occur

This checklist is meant as a starting point – it is not legal advice. Please customize and consult your government statutes, codes, laws, and policies for jurisdictionally specific requirements, risk tolerances, and procurement environments.