Top 10 Risks for GOVERNMENT CONTRACTORS

INTRODUCTION

Today's government contractors operate in an inherently risky environment—managing this portfolio of risks is especially important to ensure success. By strategically managing risk, you can reduce the chance of loss, create greater financial stability, and protect your resources to ensure that you achieve your strategic objectives and build stakeholder value.

aronson LLC
ASSURANCE | TAX | CONSULTING

http://www.aronsonllc.com/

Call Us: 301.231.6200

Table of Contents

ENTERPRISE RISK MANAGEMENT (ERM)

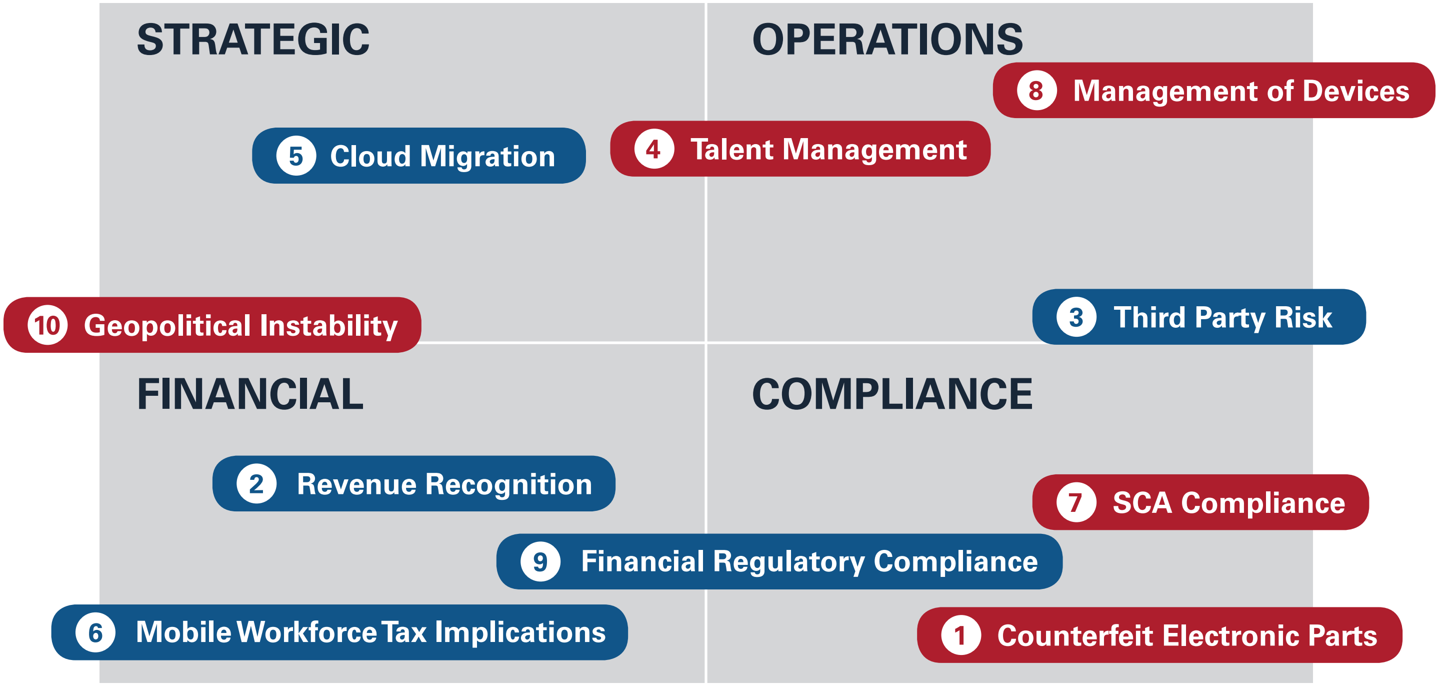
TOP 10 GOVCON RISK

Few things are more complicated than doing business with the U.S. Federal Government. In addition to the everyday issues encountered by all businesses, government contractors face unique regulatory compliance challenges at each step in the business lifecycle. Along with this risk, however, comes immense opportunity.

For more than 35 years, Aronson has focused on serving the government contracting industry. With lessons learned from our nearly 800 government contractor clients, we have gained keen insights into the competitive landscape and your business needs.

In this whitepaper, our team has highlighted emerging risks that span across the government contractor's risk universe that you need to keep on your radar. The risks we present, while not exhaustive, provides an overview of how to approach the risk discussion, understand the impact to your organization, and how you can respond.

ARONSON'S SNAPSHOT OF THE TOP 10 GOVCON RISKS BY CATEGORY



1 COUNTERFEIT ELECTRONIC PARTS

There may be no more pressing issue in government contracting than counterfeit electronic parts (CEP). It has been estimated the proliferation of CEP in the supply chain costs the government and its contractors billions of dollars per year.

In response the U.S. Department of Defense (DoD) has issued two Defense Federal Acquisition Regulation Supplement (DFARS) clauses designed to make contractors the first line of defense against CEP and, to some extent, financially liable for CEP that enter the supply chain.

The clauses, 252.246 7008 Sources of Electronic Parts and 252.246-7007 Counterfeit Electronic Part Detection and Avoidance System, will be in all DoD contracts, including service contracts, with deliverables that include electronic parts or items containing them. The exception is 252.246-7007 is not required in set-aside contracts.

252.246-7008 establishes an order of preference for obtaining electronic parts, prioritizing the original manufacturer, authorized suppliers or suppliers that obtain such parts from the manufacturer or an authorized distributer. 252.246-7007 requires contractors to maintain a risk-based CEP detection and avoidance system.

In addition to the damage CEP might cause our military personnel, 252.246-7007 states that failure of a contractor to maintain an adequate CEP detection and avoidance system may result in disapproval of the purchasing system, the withholding of payments, and the disallowance of costs related to the CEP including cost of any re-work or corrective actions required.

DoD contractors subject to these clauses should review their supply chains to determine if it includes CEP and, if so, develop a CEP detection and avoidance system commensurate with the risk. Your written policies and procedures should address the following points:

- Training
- Inspection and testing
- Traceability
- Source selection per 252.246-7008
- Reporting and quarantine
- Identifying suspect CEP
- Utilize government or industry standards
- Flow-down requirements
- Continual process improvement
- Process for screening GIDEP reports and other credible sources
- Control of obsolete electronic parts

Even contractors not subject to these clauses should implement the sourcing hierarchy set forth in 252.246-7008. Everybody is busy, but in this day and age, failure to address CEP is not an option.

2 REVENUE RECOGNITION

The new revenue recognition accounting standard (ASC 606)—the most comprehensive and disruptive accounting change to impact businesses to date—is here. Are you ready?

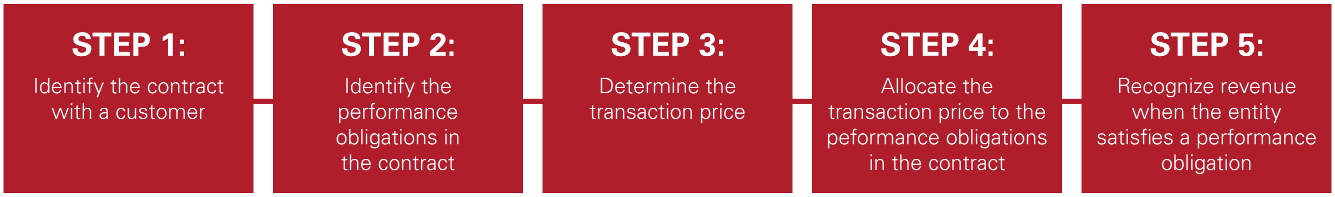
Many companies are unaware of how time-consuming and complicated adopting this new accounting standard is. Its impacts will be felt company-wide, not just within the walls of the finance and accounting department. The importance of this new standard should not be based solely on its impact or non-impact to revenue.

As a government contractor, these components are certain to cause additional complexities:

- Customer options
- Cost plus elements
- Modifications
- Working at risk
- Award-based commissions

Communication with bankers will also be critical to understand the impact to revenue projections in securing financing.

Whether using a consultant or company resources to determine the overall impacts, your company must go through the rigor of understanding, assessing, and comparing the majority revenue streams under legacy GAAP and ASC 606. This first step (of many) should be done now in order to determine and implement the changes to policies, controls, and systems.



STEP 1: Identify the contract with a customer

STEP 2: Identify the performance obligations in the contract

STEP 3: Determine the transaction price

STEP 4: Allocate the transaction price to the peformance obligations in the contract

STEP 5: Recognize revenue when the entity satisfies a performance obligation

3 THIRD PARTY RISK

Government contracting is one of the most highly regulated industries in the world. As a result, most government contractors have implemented internal controls designed to minimize the risk of non-compliance arising from the behavior of their employees. However, in this era of business process outsourcing and contracting out of other important functions to third party vendors, controls focused solely on the contractor's internal operations are insufficient to protect the contractor from compliance risk.

Although your organization may rely on third-party service providers, your management team carries the ultimate responsibility for maintaining an effective internal control system.

Non-compliance by a third party vendor is likely to be viewed by the government as non-compliance by the contractor. Taking ownership of this third-party responsibility has become one of the biggest hurdles for organizations as more and more processes move to third-party providers.

Third Party Risk Management (TPRM) is the process of analyzing and mitigating risks to your organization by parties other than your own company. Due diligence is the process by which the vendor is reviewed to determine its suitability for a given task.

Due diligence is an ongoing activity, including review, monitoring, and management communication over the entire vendor lifecycle. Having a TPRM program helps reduce the likelihood and impact of a data breach, operational failure, vendor bankruptcy, compliance violation, and reputation damage.

In order to pinpoint third party risks you first need to assess the current environment and develop a third party framework based on your organizations context. No two organizations are alike. Then develop risk stratification guidelines to highlight risks by vendor and to conduct more intense vendor assessments over the Tier 1 category. For example:

TIER 1	TIER 2	TIER 3
Critical vendors (10%)	**Major vendors (40%)**	**Vendors (50%)**
Private data + critical systems + geographical region	Private data OR critical systems OR geographical region	Commodities / low risk purchases

Items to include in your vendor assessments include:

1. Overall risk assessment
2. Financial projections
3. Insurance review
4. Background check
5. Compliance with applicable prime contract requirements
6. Legal contract review

Don't have a TPRM program yet? Below are some suggestions on how to implement internal controls now:

- When engaging vendors, ensure your evaluation process and/or Request for Proposals (RFP) includes consideration for meeting your organization's baseline internal controls standards.
- Periodically evaluate Key Performance Indicators (KPIs) of service providers with respect to service requirements indicated in the Service Level Agreements (SLAs).
- Request and review Service Organization Control (SOC) Reports and determine whether follow-up actions are necessary.

FINAL TAKEAWAY: don't decide on a vendor too early in the process. Best price does not equal best vendor (as we have all learned during the era of Lowest Price Technically Acceptable (LPTA) contracts). You should be focused on meeting your baseline control requirements.

Employ your internal audit department or outside consultant to review your TPRM process. This is not just a one-time deal. You must review this critical process again and again to ensure compliance with your program and evolve the design in today's rapidly changing environment.

4 TALENT MANAGEMENT

For professional services contractors, attracting and retaining talent is of paramount importance.

The high tech labor market in DC is competitive and likely to get more competitive and thus more expensive. Amazon's possible arrival could result in an exponential shift in the market dynamics in favor of employees.

Now is the time for contractors to review their overall approach to talent acquisition and management, especially with an eye towards the under 35 demographic. While salary is important, all aspects of the employer/employee relationship should be reviewed. Other factors include:

- Company culture
- Career growth
- Opportunities to work on different clients and/or engagements
- Regular and consistent feedback
- Learning and development
- Flexibility work arrangements

DC area services contractors that position themselves well as we approach the 2020s will be the contractors that succeed in what is sure to be a highly competitive market for skilled labor.

5 CLOUD MIGRATION

More federal contractors are migrating to the cloud given the ease of use in transitioning systems, the eased burden of managing IT infrastructure, and the availability for support around the clock.

Key cloud service providers are well known for their robust security practices, with many of the key players having obtained compliance with industry standards such as ISO 27001, SOC2/3, and FedRAMP. However, there appears to be a gap when it comes to the monitoring of key cloud providers.

Many organizations assume that once information has been successfully migrated to the cloud, there is no reason to provide additional vendor oversight. However, government contractors need to implement formal processes as they relate to vendor oversight, in particular for companies that manage sensitive data.

Reputable cloud service providers will provide clients a SOC1 or SOC2 Report at their request, which provides an overview of security controls in place to protect the service provider's systems.

It is management's responsibility to periodically request and review these reports, ensuring that the security controls in place at a third party meet the internal requirements of your organization.

6 MOBILE WORKFORCE TAX IMPLICATIONS

With government contracts often requiring services to be performed in multiple states, a service provider's workforce is becoming increasingly mobile. Combining this increased mobility with more sophisticated state audit techniques results in the need for government contractors to have clear procedures in place when their work requires employees to venture into new states.

Contractors need to regularly communicate with their income tax advisors regarding activity in new states so a determination can be made as to whether additional state income tax returns are needed. Having a nexus analysis performed by your tax advisor can be helpful for contractors with varying levels of activity across jurisdictions to ensure that the proper state returns are being filed.

States have varying rules regarding nexus, with many states enacting more aggressive standards over the last several years. For business owners looking to sell the company, state income tax noncompliance more often than not can be the cause of a deal being held up or a larger than expected holdback.

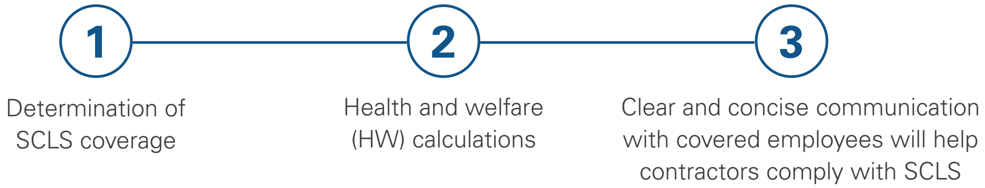
In addition to state payroll and income tax issues, certain jurisdictions with unique sales or gross receipts taxes can cause unexpected deficiencies for government contractors. All state tax types are best dealt with in a proactive manner, which means that contractors must have clear pre-contract procedures in place that address whether there are pending filing obligations for the varying state tax types.

7 SCA COMPLIANCE

No contractor is naturally compliant with the Service Contract Labor Standards (SCLS) formally and infamously referred to as SCA (Service Contract Act).

Successful compliance with SCLS involves numerous disciplines within the organization including human resources, project management, accounting, and pricing. Intentional steps must be taken to ensure full compliance with this complex regulation. Noncompliance with SCA can result in withholding of payments to pay back underpaid employees, legal action, contract termination, debarment, and even jail time.

SCLS contains many complexities, but a few best practices include:



1 Determination of SCLS coverage

2 Health and welfare (HW) calculations

3 Clear and concise communication with covered employees will help contractors comply with SCLS

The best start on the road to compliance is to determine SCLS coverage before bidding on the solicitation. Review the solicitation for incorporation of either of the two following clauses: FAR 52.222-41 Service Contract Act of 1965 or 29 CFR Part 4, Section 4.6. If the solicitation seems like it should be SCA-covered, but neither clause is included, ask the question during the Q&A phase of the proposal process.

Next, SCLS compliance boils down to ensuring that each employee receives the required minimum wages, HW, holidays, and vacation according to the incorporated Wage Determination (WD). Complying with the HW requirement is the most complicated of the four SCLS requirements mentioned above.

Contractors must determine the contract-applicable method for calculating the required HW based on whether or not the incorporated WD is odd (individual employee-by-employee calculation) or even (average calculation).

Lastly, throughout the entire performance of the contract, it is critical that contractors have clear and concise communication with SCLS employees. Not only are specific employee notifications required by the regulation, but clear communication can help to prevent Department of Labor (DOL) investigations. Compliance must be continually and actively monitored throughout contract performance.

8 MANAGEMENT OF DEVICES

With the ever-growing supply of handheld devices and systems entering our personal world, there is no question that they too will be present in the government contracting world as well.

Many organizations place significant effort and resources into managing devices (and corresponding media) on their networks, leveraging dedicated tools and technologies to ensure only authorized devices are permitted access to information systems. Others have a much more manual process and rely on strong cybersecurity training and practices organization-wide to reduce the risk of inappropriate device access or use.

Regardless of your organization's approach to device management, all need to be cognizant of all devices (whether it be a smartphone, tablet or external hard drive) that may potentially have access to your organizational information and have a strategy in place to manage these devices on an ongoing basis.

Organizations should explicitly state within their Policies and Procedures what types of devices or portable media are permitted on organizational systems, general guidelines for use, and corresponding roles and responsibilities around the management of all devices.

Although not an exhaustive list, organizations should consider the following when determining their approach to managing devices on their systems:

- Is your approach to implement a Bring Your Own Device (BYOD) policy or restrict use of devices to only those issued by your organization?
- How are devices going to be tracked, and what level of information should be kept for each record?
- Are there restrictions on the types of devices permitted on organizational systems, and restrictions on the type of information accessible to these devices?
- Do devices require specific security configurations (e.g. PIN must be enabled) prior to being granted access to organizational systems, and how are these checks to be performed?
- Has the process for adding/removing devices from organizational systems been formalized? Is there a process in place for visitors/contractors?
- Have system users received security related training regarding appropriate use of devices on organizational systems?
- Is there a process in place to deal with lost, stolen or compromised devices?

While there is no doubt that the use of handheld devices has increased productivity and collaboration amongst organizations, they also introduce additional risks to organizational information. Devices may provide entry points into organizational networks or have sensitive client information stored locally, which may result in the unauthorized disclosure of information if not properly managed or devices are compromised.

Strong controls around device management will reward organizations with peace of mind that risks related to the use of external media and devices are mitigated and provide a foundation for future growth and governance for device types.

9 FINANCIAL REGULATORY COMPLIANCE

Many contractors face increased scrutiny with more and more regulation followed by government audits of financial processes and controls.

Simply incurring a cost in support of a federal contract is not a guarantee that the cost will be reimbursed and sustained under audit. For a cost incurred to be reimbursed and sustained under audit it must meet each of the following criteria:

- Allowable in accordance with FAR Part 31 cost principles
- Allocable
- Reasonable
- Incurred in accordance with Generally Accepted Accounting Principles (GAAP)
- Allocated in accordance with Cost Accounting Standards (CAS) if applicable
- Comply with specific contract terms

Costs disallowed under government audits expose contractors to large financial risks that may not only wipe out the profit on a contract but result in a loss. Costs listed as expressly unallowable in FAR Part 31 are typically not the risk, as these costs are well known by savvy federal contractors. Such unallowable costs are excluded from estimation, segregated from accumulation of reimbursable costs and not billed on federal contracts.

The real risk under government audits is the lack of supporting documentation, evidence of reasonableness, and allocability of seemingly allowable costs at the time of the audit.

The financial compliance risk is even more disruptive to organizations as the time invested by staff during an audit and the potential reputational risk accumulate in addition to the funds due back to the government. Much of this risk can be mitigated if the proper policies and procedure are in place and followed.

Many government audits take place years after a cost is incurred by a contractor, thus accounting records with adequate documentation (including receipts and timesheets) must be kept for many, many years.

What happens when time passes and a company is acquired or there is a system conversion?

Many times, this exacerbates the risk as documents are either not maintained or organized in a manner to make them easily accessible. The adequacy and accessibility of documentation are critical as the individual who approved the cost and payment most likely will not be around at the time of the audit.

How can contractors mitigate financial compliance risks?

- Reviewing your policies and procedures for adequacy as well as the effectiveness can assist in identifying exposure and mitigating risk.
- Performing periodical reviews of the compliance with the policies and procedures allows the organization to proactively repair any gaps and provides time to locate supporting evidence. If you wait until the audit it's too late.
- Reviewing the level of documentation is also critical as the game of federal contracting is officiated well after the play is made.

10 GEOPOLITICAL INSTABILITY

Political instability, both at home and abroad, can hurt a company' profitability. Geopolitical risks are interrelated, so they need to be looked at holistically in the context of other risks. For example, weak rule of law in a region can lead to a range of risks from state failure, political violence, terrorism to high inflation and rising food prices.

Geopolitical unpredictability has become a driver of uncertainty. Understanding the influences between diverse kinds of risks is a critical step in risk mitigation. It is important for government contractors to understand the causes, trends, and situations to look out for and to prepare for the possible consequences.

What can government contractors do to mitigate geopolitical risks?

- Implement an enterprise risks management framework and reporting structure to assess and report on key strategic risks and mitigation plans to key stakeholders.
- Review for adequate insurance coverage.
- Actively work to identify supply chain disruption.
- Utilize scenario planning tools, train team members and implement early warning systems.
- Adopt big data and other data-driven management techniques.
- Conduct risk-based due diligence when acquiring foreign business entities and/or working with foreign business partners.

GOVERNMENT CONTRACTORS DRIVING VALUE WITH ERM

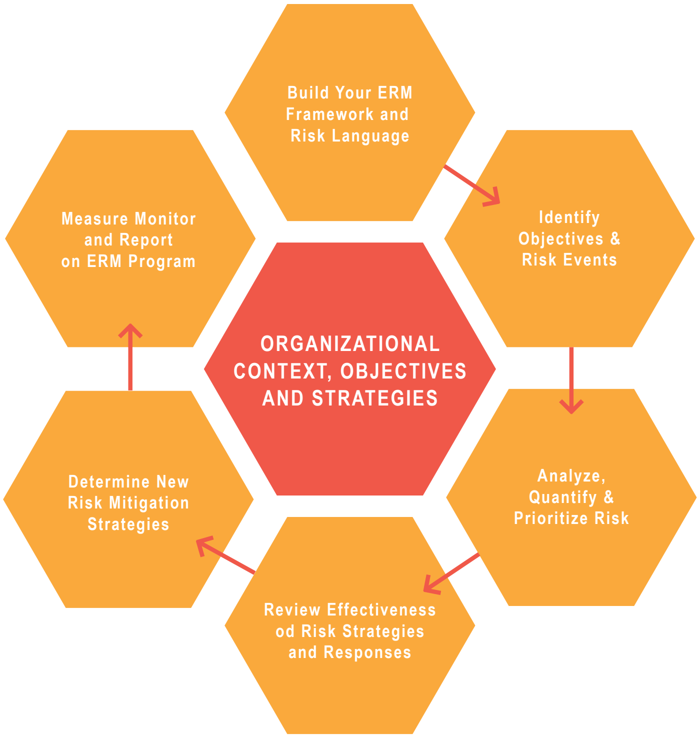
CALL TO ACTION

It's time to talk to leadership about risk to your strategy.

The Aronson Risk Advisory Approach

- *Update risk universe annually.* Your organization's risk model should be updated annually to reflect your organization's risk environment. This will be utilized as a framework to ensure that the full risk universe is considered during the risk discussions.
- *Heatmap top risk scenarios and prepare remediation plans.* Compiled risk scenarios should be ranked according to significance and likelihood of occurrence. Items above the line are candidates for further investigation, workshops, and mitigation plans.

Suggested Risk Management Structure


Build Your ERM Framework and Risk Language
Identify Objectives & Risk Events
Analyze, Quantify & Prioritize Risk
Review Effectiveness od Risk Strategies and Responses
Determine New Risk Mitigation Strategies
Measure Monitor and Report on ERM Program
ORGANIZATIONAL CONTEXT, OBJECTIVES AND STRATEGIES

Critical Success Factors

- *Develop procedures.* Create a procedure document for conducting the ERM framework and process, such as an ERM charter that answers the following questions:
  - Who is responsible for initiating and conducting risk assessments?
  - Who will participate?
  - What steps will be followed?
  - How will disagreements be handled and resolved?
  - What approvals will be needed?
  - How will the assessments be documented?
  - How will assessments be maintained?
  - To whom will the reports be provided?
- *Create standard tools* (such as questionnaires) and formalized reporting (such as heatmaps).
- *Involve business and technical experts.* Business managers generally have the best understanding of the criticality and sensitivity of business operations and of the systems and data that support these operations. Technical personnel—like IT, CPAs and Risk Advisory specialists—bring an understanding of vulnerabilities as well as knowledge of impacts, associated costs, and the controls that are implemented.
- *Formalize timing of risk reporting to leadership.* Set a standard for quarterly meeting topics and templates to be presented. Ensure it is on the meeting agenda for top management at least annually.

EXAMPLE OF GOVCON RISK UNIVERSE

STRATEGIC

Governance:

- Organizational structure
- Strategic planning
- Budgeting and forecasting

Market:

- Competition
- Geo-political
- Economic factors

Reputation:

- Organizational character
- Brand
- Product safety
- Customer service
- Media relations
- Employee communication

Stakeholders:

- Business partners
- Customers
- Suppliers
- Government

Mergers, Acquisitions & Divestures:

- Valuation and pricing
- Due diligence
- Execution and integration

Major Initiative:

- Vision and direction
- Planning and execution
- Business acceptance
- Technology implementation

COMPLIANCE

Standards of business conduct:

- Ethics
- Hotline
- Fraud and illegal acts
- Monitoring and reporting
- Training
- Policies

Legal:

- Awards and contracts
- Litigation
- HR conerns
- Environmental
- Health and safety
- Insurance

Regulatory:

- Acquisition and assistance regulations (e.g. FAR, CAS)
- Government audits
- Privacy
- Labor
- Local Laws & Regulations

OPERATIONS

People:

- Leadership
- Culture
- Labor reporting and charging
- Recruitment and retention
- Development and performance
- Succession planning
- Compensation and benefits
- Capacity Building

Process:

- Business development
- Procurement and sourcing
- Customer support
- Business continuity
- Facilities management
- Estimating and proposals
- Contract administration
- Efficiency and cycle time

Global Security:

- Assets
- People

Knowledge:

- Intellectual Property (IP)
- Intangible assets
- Information management

Technology:

- Security and access
- Availability and continuity
- Integrity
- Global infrastructure
- Platform and tools

Disaster Recovery:

- Natural events
- Terror and malicious acts
- Pandemic

FINANCIAL

Market:

- Foreign currency
- Inflation

Liquidity and credit:

- Credit and collectibles
- Cash management and forecasting

Accounting and reporting:

- Revenue recognition
- Internal controls
- Budget monitoring

Cost accounting:

- NICRA and cost allocations
- Cost allowability
- Incurred Cost Submissions (ICSs)
- Award contract billing

Tax:

- Tax strategy and planning
- Transfer pricing

ABOUT ARONSON

For more than 35 years, Aronson has focused on serving the government contracting industry. Whether you're a small, mid-size or large business, we're here to advise you on the best strategies to maximize shareholder value throughout your company's lifecycle.

In addition to traditional accounting services such as assurance and tax, we offer a full range of consulting services focused on your industry. The depth and breadth of our services ecosystem allows us to customize our approach to your business.

We can help you successfully navigate the day's most pressing issues and spot opportunities and risks on the horizon well ahead of your competitors.

Aronson's team of professionals helps organizations unlock value, strengthen decision-making, and prevent internal control failures. Contact us today.

MELISSA B. MUSSER, CPA, CITP, CISA
Director, Risk Advisory
mmusser@aronsonllc.com
240.364.2598

NICOLE M. MITCHELL, CPA, CGMA
Lead Partner
of Consulting
nmitchell@aronsonllc.com
301.222.8231

LEXY B. KESSLER, CPA, CGMA
Partner, Government
Contract Group
lkessler@aronsonllc.com
301.231.6218

PAYAL VADHANI
Partner, Cybersecurity,
Risk & Compliance
pvadhani@aronsonllc.com
301.231.6259

TOM MARCINKO
Principal Consultant,
Government Contract Group
tmarcinko@aronsonllc.com
301.231.6237

LA-TASHA S. R. PATEL, CPA
Managing Consultant,
Government Contract Group
lpatel@aronsonllc.com
301.231.6260

RENZO PORTELLA
Manager, Cybersecurity,
Risk & Compliance
rportella@aronsonllc.com
301.231.6657

MICHAEL L. COLAVITO JR., JD
Senior Manager,
Tax Group
mcolavito@aronsonllc.com
301.231.6298

BARBARA E. CONNELL
Managing Consultant,
Government Contract Group
bconnell@aronsonllc.com
240.364.2657