

CALIBRE

Cyber Security Programs

CYBER
SECURITY

NETWORK
SECURITY

DATA
PROTECTION
INFORMATION
PRIVACY

OUR SUPPORT SERVICES

- >> *Cyber Security Programs*
- >> *Data Strategists*
- >> *Contracting for Security - Supply Chain Cyber Risk Management*
- >> *Risk-Based Security Management (RBSM)*
- >> *CALIBRE's Acquisition Risk Mitigation Assessment (CARMA)*
- >> *Virtual Chief Information Security Officer (VCISO)*

CALIBRE provides a variety of cyber security services designed and tailored to suit our customers' unique operational environments, missions, and challenges. Using Risk-Based Security Management (RBSM) techniques, we provide a quantitative analysis that enables our customers to make business-justified investments for their security programs. Our expertise in security and cost management facilitates strategic investment guidance for security programs in addition to enhancing a customer's security posture and reducing the risk of potential litigation. CALIBRE's cyber security team provides support to identify threats that pose a risk to sensitive data and the confidentiality, integrity, and availability of network operations. Our subject matter experts work with our customers to enhance security posture and reduce risk, and understand the trade-offs and investments.

>> *Digital Forensics*

CALIBRE provides investigative services to support or refute civil claims of negligence associated with data breaches and lack of implemented commercially reasonable cyber security. Our specialists move quickly to work with our customers to obtain and analyze stored data. Trained in court-admissible forensic software, we closely follow evidentiary procedures according to state and federal requirements. CALIBRE thoroughly investigates the incident and works directly with your senior leadership or legal counsel. Our digital forensic services can be performed independently or after our penetration test. Our specialists prepare formal reports and on-site debriefs to your organization for future criminal or civil pursuits.

>> *Contracting for Security - Supply Chain Cyber Risk Management*

Securing our customers does not simply stop at our customers' firewalls.

Organizations in both public and private sectors use contract language that impedes value or exposes the organization to unnecessary risk. Technology advancements make it challenging for contracting officers, end-users, technology specialists, and senior management to address security concerns throughout the acquisition lifecycle process. In accordance with the President's Executive Order for Improving Critical Infrastructure Protection Sec. 8(e), CALIBRE security and contract specialists conduct an extensive review of proposed terms and conditions, service-level agreements, or procurement language to identify risks associated with cyber security and information assurance. By clearly illustrating identified risks and providing multiple recommendations for improvement, organizations obtain the highest assurance of acceptable security for legally binding agreements with their customers technology or service providers.

>> **RBSM/CARMA**

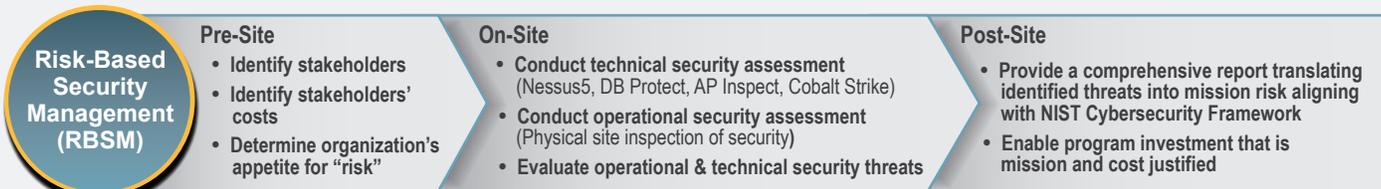
To reduce the risk of insider threats, data loss, system disruption/failure, privacy requirements violation, and other vulnerabilities commonly associated with the contractor workforce, CALIBRE proactively assesses cyber security risk to align with recent recommendations by the General Services Administration, Department of Defense, and Department of Homeland Security (GSA/DoD/DHS). Our RBSM approach enables us to quantify incident costs prior to occurrence, incentivizing stakeholders to make mission and cost-justified investments in security to align with DHS's Risk Management Framework and NIST's Cyber Security Framework. This investment guidance enables organizations to construct budgetary line item requirements to address security program investment regardless whether the goal is to enhance an

organization's "Profile" (as defined by NIST Cyber Security Framework) or with the Office of Management and Budget (OMB) Exhibits 300, 53a, and 53b - linking information technology and cyber security investments to strategic planning.

CALIBRE is actively involved in working with the Government to assess methods to reduce recently publicized risks related to critical infrastructure and secure supply chain management. We provide Independent Verification and Validation (IV&V) security assessments of organization's corporate enterprise to align with secure supply chain initiatives described in Executive Order (EO) 13636 and the Government's new Cyber security Framework.

Another key feature of our risk management approach is CALIBRE's Acquisition Risk

Mitigation Assessment (CARMA) technique, which provides an enhanced level of assurance by lowering risks known to cause organizations harm. We measure against NIST SP800-53 revision 4 controls recently defined under the Defense Federal Acquisition Requirements and evaluate what controls have the highest probability of causing a security event. We assess these controls to determine which ones have the highest likelihood of causing a formal sanction or litigation when a security event occurs. By applying RBSM and CARMA approaches, CALIBRE provides a unique and necessary vetting process that gives decision-makers new datasets to quantify and reduce risk based on cost estimation at point of threat discovery versus the cost of incident response.



Risk-Based Security Management Informs Investment Decisions. CALIBRE provides new techniques and innovative risk-based security management processes to help you evaluate and reduce risk and to focus investment decisions for security program budget justifications.



CALIBRE's Acquisition Risk Mitigation Assessment. CALIBRE's risk assessment techniques align with NIST Cyber security Framework Profile objectives, reducing risk from technical and operational threats.

>> **Virtual Chief Information Security Officer (VCISO)**

In today's market every business has an imperative to manage operational costs and investments. IT Security, Information Security, Compliance, Governance, and Risk Management are all significant and often daunting financial commitments. CALIBRE's VCISO charts a course for attaining your security and risk management objectives in a cost effective and highly efficient way. By leveraging over 25 years of data analytics, cost management, technology solutions, and decision support your business immediately enjoys a "peace of mind" knowing our

industry recognized subject matter experts will reduce your risk exposure. CALIBRE's VCISO service understands threats that exist today with inherent convergence of both cyber and operational risks. We provide our customers with scalable decision support that considers the whole cost of ownership with your security program investments. By working with a CALIBRE VCISO, you can expect sound risk discussions coupled with a quantifiable risk matrix to justify the decisions that need to be made for the success of your business and the maturity of your security program.

ABOUT CALIBRE

CALIBRE Systems, Inc. is an employee-owned management consulting and information technology solutions company supporting government and industry. CALIBRE is committed to the success of our clients and delivers enduring solutions that solve management, technology, and program challenges.

For more info contact us at info@calibresys.com