RISK MANAGEMENT FRAMEWORK SERVICES

CYBERSECURITY RISK MANAGEMENT FRAMEWORK CONSULTING SERVICES TO SUPPORT SECURE, COMPLIANT REPAIR, ADDITION, AND UPGRADE OF U.S. GOVERNMENT FACILITIES

Many government facilities and their infrastructure no longer meet the current U.S. government environmental standards, utility monitoring requirements, or physical and cybersecurity requirements. At the same time, building support facilities and automation systems have become more intelligent and more dependent upon processor-driven control. These systems require network access for facility monitoring, energy management, and integration into base micro-grid systems and present a much broader cyber-attack surface than traditional infrastructure. Peraton Labs supports the efficient and secure repair, addition and upgrade of U.S. government facilities by incorporating the cybersecurity Risk Management Framework into the architecture and engineering process from initial facility design through achieving cybersecurity approval via an Authorization to Operate.

Peraton | LABS

THE CHALLENGES

Many government facilities were constructed over 25 years ago and their infrastructure no longer meets the current U.S. government environmental standards, utility monitoring requirements, or physical and cybersecurity requirements. Often mechanical, fire protection, electrical distribution, security systems, and other building infrastructure must be upgraded to support new operational needs and facility repurposing.

Military Facility Upgrade Challenges

- Facility repurposing
- Environmental monitoring requirements
- Risk management requirements

At the same time, building support facilities and automation systems have become more intelligent, more dependent upon processor-driven control, and reliant upon firmware patching and network access for facility monitoring, energy management and integration into base micro-grid systems. Known as Industrial Control Systems (ICS), these cyber-physical systems present a much broader cyber-attack surface than traditional infrastructure and must be protected for mission assurance.

The U. S. Government has steadily increased its security requirements for ICS, building automation, life safety, utility monitoring and base control systems, bringing them under the Risk Management Framework process with DoD Unified Facilities Criteria (UFC) 4-010-06 and Unified Facilities Guide Specifications (UFGS) 25 05 11.

PERATON LABS SOLUTION

This white paper describes Peraton Labs approach to incorporate cybersecurity Risk Management Framework (RMF) into the architecture and engineering (A-E) process to support initial facility design through achieving cybersecurity approval via an Authorization to Operate (ATO). Our approach includes all cybersecurity measures and controls as applicable to the communications, computer, and control systems, devices, and networks to provide the appropriate Confidentiality, Integrity, and Availability (CIA) impact level (low, moderate, high) for each device and network application. The RMF, as applicable to UFC 4-010-06, UFGS 25 05 11, and other applicable government cybersecurity requirements are incorporated into the cyber design and applicable engineering deliverables (drawings, outline specifications, DA, cost estimate, etc.).

DECADES OF EXPERIENCE

Peraton Labs has decades of government cybersecurity and RMF process experience with both unclassified and classified projects. Our Information Systems Security Officers (ISSO) have expertise in developing artifacts, assigning controls, demonstrating compliance, and achieving ATO for owned infrastructure and cloud-based solutions. Our ISSOs support the entire accreditation lifecycle and security engineering activities from the base system design -- guiding development teams on applicable Information Technology (IT) and Operational Technology (OT) control requirements, including AR 25-2, DODI 8500, NIST SP 800-53, DoD Security Technical Implementation Guides (STIGs), and CNSSI 1253 security requirements at all sensitivity levels. For the OT UFC and UFGS mentioned above, Peraton Labs uses the Intelligence Community Standards 705-1 and 705-2 along with Department of Defense Manual 5200.01 volume 3 for construction and management in our Sensitive

Peraton Labs Risk Management Framework Solution

- Decades of experience
- Design & Charette support
- Define RMF scope
- Stakeholder relationships
- Risk tolerance
- Define cybersecurity architecture
- RMF package preparation
- Service value

Compartmented Information Facilities in 5 company CONUS locations. Post initial deployment, our ISSOs create and manage Continuous Monitoring control activities, ATO Change Requests, FISMA reports, Continuity of Operations (COOP) periodic reviews, and Certification yearly reviews. We conduct verification testing and produce risk assessments for the solution based on test results.

DoD Instructions 8500.01 and 8510.01 define the Risk Management Framework (RMF) and establish a category for ICS or “special purpose” systems that are not traditional information technology, called Platform Information Technology (PIT) systems. PIT systems, which include ICS, use specifically tailored security controls sets and require the cybersecurity architect to have expertise in the system.

A successful government construction project now requires the discipline of cybersecurity to take a seat at the table with the architects, engineers, and trades to contribute to the facility design to minimize potential cyber risks, suggest alternatives and compensating solutions, and provide guidance to eliminate unnecessary features that may create additional cybersecurity burden and project cost. Peraton Labs provides the following RMF consulting services to support the end-to-end A-E process for facility renovation, rebuilds, and upgrade projects.

DESIGN AND CHARRETTE SUPPORT

- Participate in the on-site/remote facility investigation A-E meetings and attend design Charrette meetings with the customer stakeholders to represent the project cybersecurity requirements, begin identifying the systems that will be subject to RMF, and ensure the project plan and budget appropriately reflect the needed activities, milestones, resources, and schedule to achieve ATO.
- Participate in meetings with the System Owner and Authorizing Official to understand the Confidentiality, Integrity, and Availability impact levels assigned to facility systems.

DEFINE RMF SUPPORT

Define the RMF activity scope by identifying all facility assets, building controls and automation, environmental support, and communications systems that require cybersecurity consideration and require RMF documentation as addressed in design and Charrette meetings. This activity includes identifying all cybersecurity requirements by Common Control Identifiers.

STAKEHOLDER RELATIONSHIPS

- Establish relationships with the site security officers to understand security priorities, special, site-specific cybersecurity considerations, and cybersecurity CIA requirements for the project.
- Research and investigate the proposed systems, review the vendor documentation, and speak with the product vendors to understand the capabilities and limitation of their equipment. Suggest alternative equipment or product features to best support the site’s needs.

RISK TOLERANCE

Based on the mission and function of the control system, identify each system’s risk level by assessing its Confidentiality, Integrity, and Availability impact (LOW, MODERATE, or HIGH).

DEFINE CYBERSECURITY ARCHITECTURE

- Define and convey an overall cybersecurity strategy and architecture to be included in the site design. Apply inherited security controls where appropriate to reduce project costs. Using the impact levels, identify and document the cybersecurity controls NIST SP 800-82 to be applied to each component. The determination of cybersecurity risk reduction must also consider any risks to system functionality due to application of the security controls.
- Prepare or support the creation of the system cybersecurity configurations and conduct control-based validation and vulnerability testing.

RMF PACKAGE PREPARATION

- Support preparation of the RMF package including all necessary artifacts for the components. Document the Control Correlation Identifier list for each of the singular, actionable statements that comprise a security control.
- Ensure cybersecurity design considerations are incorporated in all applicable A-E deliverables.
- Review the RMF package as prepared by A-E with the residing ISSOs and related

stakeholders. Identify and direct any needed modifications to the RMF package.

- Provide support for submitting the RMF package for government approval and ATO. Modify the RMF package and develop appropriate Plan of Action and Milestones (POAM) to address Security Control Assessor and ATO review comments for resubmission, as required.

RESOURCES

- Information assurance and compliance - Peraton Labs
- Network migration and modernization - Peraton Labs

CONTACT US

For more information on Peraton Labs' RMF service offerings, including Rough Order of Magnitude pricing, contact:

Stan Pietrowicz
Director, Applied Cybersecurity and Network Modernization
+1 732-740-1021
331 Newman Springs Road, STE 241
Building 2, 4th Floor
Red Bank, NJ 07701-6770

LEARN MORE AT

PERATONLABS.COM

150 Mount Airy Road
Basking Ridge, NJ 07920