Risk Management Framework

Several policies, regulations, and directives mandate federal agencies follow the Risk Management Framework (RMF), which addresses security controls necessary to manage organizational risk.

RMF is more than the singular practice of identifying, assessing, controlling, and mitigating risks. RMF engages the acquisition and engineering processes throughout the engineering lifecycle to determine the threat landscape, identify potential exposures, define the quantitative and qualitative risk tolerance and limits, and isolate and control the defense against potential and known vulnerabilities.

Leidos has an established history with RMF, and we work with customers to apply our lifecycle cybersecurity and engineering assurance processes based on checklist precision, responsibility and schedule alignment, and an informed knowledge base. Leidos offers comprehensive RMF services to provide rapidly tailorable processes and tools to select, implement, assess, and continuously monitor controls to help protect federal information systems and organizations. We provide an effective and efficient method to report and communicate risk-based information and risk-related decisions to officials at all levels of the federal government.

OUR APPROACH

Leidos tailors its approach for agencies to provide compliance with federal and departmental requirements, policies, directives, instructions, and memoranda. Working with civil, defense, and national security agencies, we manage security, privacy, and supply chain risks using the RMF to provide essential activities at the organization, mission and business process, and information system tiers. This includes:

- Determining the impact of any compromise of confidentiality, integrity, and availability
- Categorizing the confidentiality, integrity, and availability levels
- Selecting, tailoring, and documenting the security controls necessary to protect the system
- Developing and coordinating security-relevant artifacts
- Implementing and coordinating the security controls
- Assessing and coordinating the assessment of the effectiveness of controls and operations
- Implementing, coordinating, and supporting change management controls
- Developing and monitoring plans of action and milestones
- Providing the Authorizing Official (AO) accurate residual risk details to support an authorization to operate (ATO) decision
- Continuously monitoring security controls and reporting the security state

We provide a rapidly deployable, repeatable, risk-based process that integrates security and risk management activities into the system engineering lifecycle, including development, maintenance, sustainment, and retirement phases.

Leidos has also developed a Risk and Privacy Management Acceleration Playbook (RAPMAP) to provide guidelines to consolidate thousands of pages of standards, guidelines, practices, and informative references to process workflows, standard operating procedures, templates, and cultural values that are necessary to accomplish RMF milestones. RAPMAP rapidly allows Leidos to implement a consistent, dynamic, and flexible approach and effectively manage information security, supply chain, and privacy risks in diverse environments—accounting for complex and sophisticated threats, changing missions, and system vulnerabilities. RAPMAP's steps and tasks can be applied to developing and existing systems and may be inserted at any RMF step.

PROVEN SUCCESS

Leidos is a recognized leader in cybersecurity across the federal government, bringing more than a decade of experience defending cyber interests globally and delivering advanced capabilities honed from protecting some of the world's most valuable assets. Leidos has led transformations for three of the four largest federal government SOCs and more than 20 geographically dispersed Fortune 500 commercial SOCs.

FEATURES AND BENEFITS

Leidos tailors our services to meet the unique requirements of federal civilian, defense, and national security systems. Our RMF expertise allows us to deliver three primary benefits:

1. Rapidly and consistently create and maintain the artifacts required to demonstrate compliance with federal and organizational policies and assist risk determination and acceptance decisions by AOs
2. Help security staff identify and prioritize actions to reduce cybersecurity risk rapidly, consistently, and with less training
3. Promote near real-time risk management and ongoing system and control authorization through continuous monitoring

WHY PARTNER WITH LEIDOS?

Gleaning best practices from our work across government agencies, Leidos delivers comprehensive RMF services to ensure security and privacy requirements are satisfied for information systems or organizations. Years of experience and in-depth expertise position Leidos as a trusted partner in risk management.

NEXT STEPS

Leidos' services allow organizations to capture required documentation and complete activities in advance of an ATO activity, increasing likelihood of a successful ATO being issued. Following ATO, compliance and risk management efforts continue. While compliance alone does not ensure network security, it is a foundational element of all successful security programs.

Leidos also effectively and efficiently protects enterprises against known threats using IonIA, a proven remediation methodology that applies the right people, process, and tools. Initially developed to protect a Department of Defense IT environment, IonIA delivers more than 99% of cyber hygiene goals through better situational awareness, prioritized remediation efforts, and lower cost. Contact us to discover how our RMF or information assurance experts can help protect your systems.

FOR MORE INFORMATION

leidos.com/cyber | leidos.com/contact

Export eTrace record 20371 | 19-0052 | Leidos Creative

leidos