Security Program Management for CMMC2

RSI will develop and align your IT operations and cybersecurity practices with the Cybersecurity Maturity Model Certification requirements, validating the organizations ability to safeguard sensitive information and meet the standards mandated by the Department of Defense.

RSI's security program management activities involve the planning, implementation and oversight of your CMMC2 compliance initiatives.

Delivering 24×7 Live
US-Based
Technical Support

Getting Ahead. Staying Ahead.

Contact us today if you are interested in modernizing your IT operations and strengthening your security posture.

Renaissance Systems, Inc.

512-600-3200 | rsitex.com
sales@rsitex.com

Assess. Remediate. Maintain.

A. ASSESSMENT

Ongoing Assessment – CMMC2

- Conduct ongoing assessment of organization's information security controls and practices against the CMMC2 requirements.
- Perform interviews with relevant personnel to gather information and insights.
- Assess the effectiveness of security measures, data protection practices, access controls, and incident response procedures.
- Identify and assess potential security risks and vulnerabilities.
- Evaluate the organization's handling of Controlled Unclassified Information (CUI).

Recommendations & Roadmap

- Provide a detailed report outlining the identified gaps and non-compliance areas.
- Offer specific recommendations and best practices for addressing the deficiencies.
- Develop a roadmap for achieving CMMC2 compliance, including timelines and action items.
- Discuss the potential security enhancements and their impact on the organization

B. POLICY DEVELOPMENT

- Establish comprehensive security policies and procedures that align with CMMC2 requirements.
- Review and update current policies where needed

C. INCIDENT RESPONSE PLANNING

- Develop a robust incident response plan to address security incidents promptly and effectively.
- Thorough assessment of organizational assets, identification of potential threats, and the development of a detailed, actionable plan. This encompasses creating response procedures, defining communication protocols, conducting tabletop exercises, and continuous refinement to ensure readiness for rapid and effective response to any cybersecurity incident.

D. SYSTEM SECURITY PLAN (SSP) DEVELOPMENT

- Develop a comprehensive document that outlines the security controls and safeguards implemented in the organization.
- Includes conducting a thorough assessment of existing security controls, collaborating with key stakeholders to identify system components, documenting security policies and procedures, and crafting a robust SSP that outlines risk management strategies, security measures, and continuous monitoring processes to ensure ongoing compliance with CMMC2 requirements.

E. PLAN OF ACTION & MILESTONES (POAM) TRACKING

- Document and manage the remediation of weaknesses or deficiencies identified in an information system's security controls.
- Detail the specific actions or strategies that will be taken to address each weakness.
- Includes identifying and prioritizing security weaknesses, proposing corrective actions, establishing realistic milestones, and providing a comprehensive roadmap for the systematic implementation of security measures to address vulnerabilities and enhance the organization's overall cybersecurity posture.

F. GOVERNANCE

- Ensure that the security program aligns with CMMC2 requirements.
- The scope includes the establishment of governance structures, regular compliance assessments, and the facilitation of communication channels to promote a culture of security and regulatory adherence.

G. COMMUNICATION & REPORTING

- Provide regular updates to senior management and stakeholders on the status of the security program.
- Project plan with timelines and milestones.
- Assessment findings report with prioritized gaps and deficiencies.
- Recommendations report with a compliance roadmap.
- Final assessment report with refined recommendations and action plan.
- System Security Plan and Plan of Action & Milestones

ABOUT RSI

Since 1982, RSI has served business of all sizes and industries with turn-key communications and IT solutions with proven results. RSI is a leading nationwide provider of:

- Core ti edge IT solutions
- Cybersecurity
- Cloud Migrations
- Live Technical Support
- Risk Assessment (HIPAA, NIST, NYS, DFS, etc)
- Business Continuity and Disaster Recovery Plans
- Comprehensive Internal & External Penetration Testing