

Position Summary

Avum is seeking a Cybersecurity Specialist to support Risk Management Framework (RMF), security compliance, and system authorization activities across Federal and Department of Defense (DoD) programs, including systems operating in Impact Level 6

(IL-6) environments.

This individual will support security assessments, maintain authorization documentation, coordinate vulnerability remediation, and help ensure systems meet applicable DoD security requirements. The ideal candidate has hands-on experience supporting DoD RMF and Authority to Operate (ATO) activities and can work closely with system administrators, engineers, program managers, and security stakeholders.

Key Responsibilities

- Support RMF assessment, authorization, and continuous monitoring activities for Federal and DoD systems, including systems operating in IL-6 environments.
- Support the implementation, assessment, and maintenance of security controls in accordance with NIST SP 800-53, DoD RMF, and applicable program requirements.
- Develop and maintain ATO package artifacts, including System Security Plans (SSPs), security control implementation statements, assessment evidence, and Plans of Action and Milestones (POA&Ms).
- Maintain security control records, supporting evidence, assessment findings, and authorization documentation in eMASS or other program-designated systems.
- Conduct security assessments, vulnerability reviews, and compliance evaluations.
- Review ACAS vulnerability scan results, SCAP outputs, and Security Technical Implementation Guide (STIG) compliance findings, as applicable to the environment.
- Coordinate remediation activities with technical teams, track findings through resolution, and maintain documentation supporting closure.
- Support compliance with applicable DoD Cloud Computing Security Requirements Guide requirements for IL-6 environments.
- Perform continuous monitoring activities, maintain security status records, and prepare required cybersecurity reports.

- Evaluate system changes for security impact and identify necessary updates to controls, assessments, and authorization documentation.
- Support security audits, inspections, and customer assessments.
- Work with technical and security stakeholders to identify, document, and mitigate cybersecurity risks.
- Support incident response and security investigations as needed.
- Stay current on evolving cybersecurity threats, regulations, and applicable DoD security requirements.

Compensation

The salary range for this position is \$110,000 to \$145,000 annually. Actual compensation will be determined based on experience, qualifications, certifications, and geographic location.

Avum offers a comprehensive benefits package including medical (Cigna), dental and vision (Principal), 401(k), PTO, education reimbursement, and certification reimbursement.

Work Environment & Requirements

- Hybrid/remote work environment with potential on-site requirements based on contract needs
- U.S. citizenship required.
- Active Secret security clearance or the ability to obtain and maintain one, consistent with contract requirements. An appropriate active clearance and authorized access are required before performing classified duties.
- Background investigation required.

Equal Employment Opportunity

Avum, Inc. is an Equal Opportunity Employer. All qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, national origin, disability, veteran status, or any other protected class under federal, state, or local law. Avum is committed to compliance with Section 503 of the Rehabilitation Act and VEVRAA, and maintains an active Affirmative Action Plan.

Required Qualifications

- Bachelor's degree in Cybersecurity, Information Technology, Computer Science, Information Systems, or a related field. Equivalent experience may be considered.
- Five or more years of experience supporting Information Assurance, Cybersecurity, or Information Security programs.
- Experience supporting DoD RMF and ATO activities, including security control documentation, assessment support, POA&M management, and continuous monitoring.
- Working knowledge of NIST SP 800-53 security controls and DoD RMF processes.
- Experience developing and maintaining SSPs, security control implementation statements, assessment evidence, and other authorization documentation.
- Experience using eMASS or a comparable system to maintain RMF records and authorization artifacts.
- Experience reviewing vulnerability scan results and STIG compliance findings and coordinating remediation with technical teams.
- Understanding of security requirements for classified systems and cloud environments.
- Strong analytical, organizational, and communication skills.
- Ability to work collaboratively with technical teams and manage multiple security documentation and remediation priorities.
- Ability to meet applicable contract-specific DoD 8140 qualification requirements for the assigned cybersecurity work role.
- Preferred Qualifications

Active Secret security clearance.

- Experience supporting DoD IL-6 cloud environments or other classified DoD systems.
- Familiarity with the DoD Cloud Computing Security Requirements Guide and its application to IL-6 environments.
- Hands-on experience with ACAS, SCAP, STIG assessment tools, and related cybersecurity technologies.
- Experience supporting cloud security initiatives within AWS or Azure, particularly government or classified environments.
- Relevant security certifications such as Security+, CISSP, CGRC, CISM, or SecurityX.
- Familiarity with CNSSI 1253 and security control requirements for national security systems.