|  |  |  |  |
| --- | --- | --- | --- |
| **Job ID :** | RS143940 | **Job Title** | Cybersecurity GRC Engineer |
| **Project Start Date :** | 02-24-2025 | **Position Type :** | Contract |
| **Project End Date :** | 08-25-2025 | **Client :** | Network Security |
| **No.of Positions :** | 1 | **Primary Skills :** | Content Strategy Planning |
| **Location :** | Dallas, TX | **Remote Work :** | None |
| **Talent must reside at location on submission?** | Yes | **Send Resumes to :** | resumes@taurusbiz.com |
| **Level/Salary Range :** | $42/hr on W2 |  |  |
| **Description :**  Engineer, GRC &amp; Assessments (ANSP Program)  FOCUS  • Ensure secure aircraft, ground, and communications systems relied upon for our ANSP Program, with concentrated attention towards risk, governance, vulnerability management, policies, and standards.  **RESPONSIBILITIES**  • Develop and implement security policies and standards, ensuring compliance with industry regulations and best practices.  • Conduct risk assessments and vulnerability assessments to identify1 and mitigate security risks.  • Manage the vulnerability management program, including vulnerability scanning, penetration testing, and remediation.  • Develop and deliver security awareness training programs.  • Collaborate with stakeholders to integrate security considerations into the design and development of new aviation systems.  • Stay informed about emerging threats and vulnerabilities in the aviation industry.  **TOP SKILLS:**  **Minimum 3 years hands-on experience on below stack:**  1. Risk Management Frameworks: (e.g., NIST RMF, NIST CSF, ISO 27005)  2. Risk Assessment Methodologies: (e.g., NIST 800-30, Threat Modeling)  3. GRC Platforms: (e.g., ServiceNow GRC, RSA Archer)  4. Vulnerability Management Tools: (e.g., Tenable Nessus, Tanium)  **SKILLS:**  • Cybersecurity Risk &amp; Governance Expertise: Requires 3-5 years of progressive cybersecurity engineering experience with a deep understanding of risk management frameworks (NIST SP 800-37, ISO 27005), governance principles, vulnerability management, and security policy development.  • Risk Assessment &amp; Mitigation: Proven experience conducting risk assessments (NIST 800-30, NIST CSF), identifying vulnerabilities, analyzing threats, and developing effective mitigation strategies.  • Vulnerability Management Program Expertise: Expertise in vulnerability management tools and processes, including vulnerability scanning, penetration testing coordination, vulnerability prioritization, and remediation tracking.  • Policy & Standard Development & **Implementation:** Strong ability to develop, document, and implement security policies, standards, and procedures that align with industry best practices, regulatory requirements, and risk tolerance  • Communication & Stakeholder **Collaboration:** Excellent communication (written and verbal) and interpersonal skills to effectively communicate security risks, governance strategies, and policy recommendations to diverse stakeholders, including technical teams, management, and external partners.  **PREFERRED CERTIFICATIONS:**  • CISSP (Certified Information Systems Security Professional)  • CISM (Certified Information Security Manager)  • CISA (Certified Information Systems Auditor)  • CRISC (Certified in Risk and Information Systems Control)  • CompTIA Security+  **TOOLS AND TECHNOLOGIES:**  • Risk Management Frameworks: (e.g., NIST RMF, NIST CSF, ISO 27005)  • Risk Assessment Methodologies: (e.g., NIST 800-30, Threat Modeling)  • GRC Platforms: (e.g., ServiceNow GRC, RSA Archer)  • Vulnerability Management Tools: (e.g., Tenable Nessus, Tanium)  • Penetration Testing Understanding: (Familiarity with tools &amp; methodologies for report interpretation)  • Policy &amp; Collaboration Tools: (e.g., SharePoint, Microsoft Teams, Policy Management Platforms) | | | |
|  | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Reviewed By**: | Swathi G | **Date**: | 02/18/2025 |
| **Approved By**: | Ram S | **Date**: | 02/18/2025 |
| **Last Updated By**: | Swathi G | **Date/Time**: | 02/18/2025 |