

CLIENT'S NAME

 Torrance, California 12345 |  123.456.7890 |  resumewriter@gmail.com

AREA OF FOCUS: **CYBERSECURITY**

*Project Management | Risk Assessments | IT Governance | Source Code Analysis | Security Design and Baselines
NIST Cybersecurity Framework | ACAS and Nessus Vulnerability Scanning | STIG's/SRG's/SCAP Scanning
Escalation Management | Technical Writing and Documentation | Organizational Leadership*

QUALIFICATIONS PROFILE

Highly analytical, solutions-focused, and astute professional, with extensive IT experience and proven background in managing and mitigating cybersecurity vulnerabilities in various server systems and network infrastructures across varied data center operations. Equipped with subject matter expertise in system security, access control, and authorization as well as NIST cybersecurity framework in providing analysis and security log data from a large-scale network and security devices. Adept at performing risk assessments and audits, as well as configuring and implementing risk management framework and system security solutions to drive and guarantee high availability and optimum performance. Effective at building consensus, providing technical guidance to senior management, as well as leading and motivating teams to ensure project success.

PROFESSIONAL EXPERIENCE

COMPANY NAME

Senior Risk Management Specialist/Subject Matter Expert

Jul 2021–Present

- Exemplify industry expertise in serving as an SME in the DISA Cloud Computing Program Office (CCPO) for the ongoing implementation of RMF for multiple commercial cloud-based systems (Microsoft Azure, Amazon AWS, and Google Cloud Platform)
- Function as a senior cyber security technical advisor for the government in charge of overseeing the DoD wide-cloud effort
- Chair technical discussions with government and contracted personnel from disparate backgrounds, while communicating the department-wide goals and strategy into actionable requirements
- Implements Agile-Scrum Development methodologies for project management.
- Initiate an Agile approach to instigate RMF and FedRAMP requirements against approved commercial clouds environments, such as SaaS, PaaS, and IASS
- Steer efforts in integrating new plans, designs, and systems into ongoing DevSecOps environments

COMPANY NAME

Senior Cyber Architect and Engineer

Sep 2019–Present

- Oversee deadlines and schedule completion dates for the V-Department Risk Management Framework (RMF) packages
- Deliver cybersecurity testing and security control validation for the Naval Surface Warfare Center Dahlgren Division (NSWCDD) V-Department
- Perform security controls analysis in accordance with the security assessment plan and the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev4 assessment procedures
- Design architectural and technical documentation measuring the actual accreditation boundary
- Earned a collective ingenuity award through the successful acquisition of two authorities to operate (ATOs) for the V-Department within the most difficult working environment and limitations due to Covid-19

COMPANY NAME

Navy Qualified Validator II

Apr 2018–Aug 2019

- Led the implementation of the RMF for multiple systems which involved evaluating the past performance of a DoD contract proposal
- Expertly handled the Navy Expeditionary Combat Command (NECC) N7 RMF project by creating the project charter which defined the problem statement, project goals, funding, period of performance, client, deliverables, project milestones, scope, assumptions, risks, and dependencies
- Managed all stakeholders and planned engagements to enable access to the client and provide updates on the progression of the project
- Facilitated high-level briefs for the client interpreting the cyber security deficiencies and delivered direction for improvement

CLIENT'S NAME

 Torrance, California 12345 |  123.456.7890 |  resumewriter@gmail.com

- ☑ Spearheaded project tasking and project knowledge that involved defining activities from sequenced to estimated activity durations

COMPANY NAME

Senior Information Systems Security Manager

Jul 2017–Apr 2018

- ☑ Led the development and implementation of the Defense Contract Management Agency (DCMA) IA program, while providing information security technical support in the area of cybersecurity and assessment and authorization (A&A) to high-level government officials
- ☑ Rendered security oversight for four programs within DCMA and subordinate commands, and assisted with DCMA security measures, analysis, periodic testing, evaluation, verification, accreditation, and the review of information system installations
- ☑ Administered approximately 30 to 400 assets across all four programs
- ☑ Played a key role in ensuring all Information System Security Officers (ISSOs) received the necessary technical or management cybersecurity training, education, and certifications required to carry out their respective duties
- ☑ Maintained system users in compliance with DoD 8570 compliant and ensured completion of training and certifications for DCMA cybersecurity workforce personnel

COMPANY NAME

Information Systems Security Manager

Jul 2017–Apr 2018

- ☑ Contributed to the development of a proposal for a DoD contract that was up for recompet
- ☑ Displayed competency in delivering cybersecurity analyst support for the Naval Air Warfare Center Weapons Division (NAWCWD), while collaborating with various clients and the Command Information System Security Manager (ISSM) to strengthen new cybersecurity policies, disciplines, and practices required by the Navy and DoD
- ☑ Developed written Risk Management Framework (RMF) validation strategies in support of NAWCWD using acceptable practices, processes, and approaches based on NIST Special Publication (SP) 800-53A

EDUCATION

Bachelor's Degree | University Name and Address

CERTIFICATION

- Project Management Professional (PMP), Valid Until: Sep 2024
- Certified in Risk and Information Systems Control (CRISC), Valid Until: Feb 2024
- Certified Associate in Project Management (CAPM), Valid Until: Jan 2024
- CompTIA Security+, Valid Until: Oct 2023
- CompTIA Network+, Valid Until: Oct 2023
- Certified Ethical Hacker (CEH); Received: Inactive
- Certified Information Systems Security Professional (CISSP), Inactive

TECHNICAL SKILLS

Project Management:	Project Management Integration Project Scope Management Project Schedule Management Project Resource Management Project Communications Management Project Risk Management Project Stakeholder Management
Frameworks:	Federal Risk and Authorization Management Program (FedRAMP) National Institute of Standards and Technology (NIST) Risk Management Framework COBIT 5
Assessment & Authorization:	Plan of Action and Milestones (POA&M) Risk Assessment Reports (RARs) Security Assessment Reports (SARs) System Life Continuous Monitoring (SLCM) Hardware/Software Listing
Software/COTS/GOTS:	Nessus/Assured Compliance Assessment Solution (ACAS) Enterprise Mission Assurance Support Service (eMASS)/Host Based Security System (HBSS) Security Technical Implementation Guides (STIG's)/Security Requirement Guides (SRG) Security Content Automation Protocol (SCAP) Group Policy/Registry
Operating Systems:	Unix Linux Windows