Name: Jessica Rojas

Contact Information:
Email: cuevasjessica40@yahoo.com
Phone: (435)-224-3262
LinkedIn: https://www.linkedin.com/in/jessica-rojas-33212918a

Professional Summary:
Enterprise Systems Manager and Cybersecurity Professional with expertise in risk assessments, tailored security solutions, compliance, CMMC, and ISO 27001 audits. Possessing an active Security Security Clearance, adept at RMF and GRC, and skilled in aligning cybersecurity with quality management.

Education:
Master of Cyber Security and Information Assurance, Western Governors University
Bachelor of Computer Science / Minor of Military Science, Weber State University

Certifications:
Certified Information Systems Security Professional, ISC2
Security+, CompTIA
Certified Ethical Hacker, EC-Council
Certified Encryption Specialist, EC-Council

Professional Experience:
Enterprise Systems Manager - Gauss Management Research & Engineering Inc (July 2024 – Present)
- Infrastructure Management
    - Oversee the installation, configuration, and maintenance of the organization's infrastructure, including servers, networks, and storage systems.
    - Ensure high availability, scalability, and reliability of systems.
    - Manage support and service desk operations to provide timely and effective technical support to end-users.
    - Develop and implement policies, procedures, and best practices.
- Information Security Management
    - Led GMRE's enterprise CMMC Level 2 certification program end-to-end, directing technical control implementation, compliance governance, audit evidence strategy, and C3PAO coordination, resulting in successful third-party certification and maximum SPRS score of 110/110.
    - Develop and implement an information security strategy to protect the organization's data and assets.
    - Conduct risk assessments and vulnerability analyses to identify potential security threats.
    - Establish and enforce security policies, procedures, and standards.
    - Oversee the deployment and management of security tools (e.g., firewalls, intrusion detection systems, antivirus software).
    - Lead incident response efforts and conduct investigations for security breaches.
    - Ensure compliance with relevant regulations and standards (NIST 800-171, CMMC, ISO 27001).
- Project Management
    - Plan and manage projects, ensuring they are delivered on time, within scope, and budget.
    - Coordinate with stakeholders to define project requirements and objectives.
    - Prepare project plans, allocate resources, and track progress.
    - Communicate project status and outcomes to senior management and other stakeholders.
- Strategic Planning and Budgeting
    - Contribute to the development of the department's strategic plan.
    - Prepare and manage the budget, ensuring cost-effective use of resources.
    - Evaluate emerging technologies and recommend their adoption to improve business processes.

Cybersecurity Analyst - Gauss Management Research & Engineering Inc (April 2022 – July 2024)
- Conduct comprehensive risk assessments and analyze security vulnerabilities to identify potential threats.
- Develop and implement customized security solutions to mitigate risks and enhance protection.
- Monitor security events and incidents to ensure the security and compliance of critical systems and data.
- Utilize security tools and technologies including firewalls, intrusion detection and prevention systems, and SIEM.
- Lead incident response and investigations, identifying root causes and recommending effective remediation strategies.

- Spearheaded the development of information security management system policies and procedures.
- Contributed to the information security risk management process, aligning with ISO 27001, NIST 800-171, NIST 800-57, and specific DFARs.
- Support the development and maintenance of System Security Plans (SSP) to ensure compliance and security readiness.
- Managed unclassified system vulnerabilities, implementing automated patching and real-time threat monitoring, including zero-day threats.
- Provided configuration management for information system security software, hardware, firmware, and networking components.
- Led the development of a streamlined FSO system for visit requests and foreign travel.
- Enhanced the insider threat program, strengthening organizational security posture.
- Collaborated on CMMC preparation initiatives, ensuring readiness for compliance requirements.
- Report to the executive team on IT operations, security posture, upcoming projects and audits; advise appropriate leadership of changes that can affect the security posture of the organization.
- Managed ISO 27001 audits, ensuring effective coordination of all components and facilitating successful audit processes.
- Collaborated with the quality team to assist in the ISO 9001 audit, ensuring alignment of cybersecurity practices with overall quality management.

Previous Professional Experience:
Cyber Mentor II, Cyber Security, Amazon Career Choice – FullStack Academy (January 2024 – Present)
Teaching Assistant – 2U, Trilogy (October 2022 – March 2023)
Full-Stack Developer - Gauss Management Research & Engineering Inc (June 2021 – March 2022)
Associate Full-Stack Programmer - Weber State University (March 2020 – June 2021)
Military Police - Utah Army National Guard (June 2015 – June 2022)

Desirable Qualifications and Skills:
- ISO 27001 Audit Compliance
- Vulnerability Analysis
- Risk Assessment / Management
- Incident Response and Management
- Programming: JavaScript, Java, HTML, Python, C++, PHP, SQL
- Regulatory Compliance: NIST 800-57, NIST 800-171, ISO 27001, DFARs, CMMC.
- Active Security Clearance (Secret)
- In-depth knowledge and practice of the Risk Management Framework (RMF) process.
- Extensive familiarity with DoD, Federal, and NIST Guidance, ensuring compliance with information security standards.
- Security Policies and Procedures development.
- Security Auditing and Assessment.
- Documentation and reporting for security policies risk assessments, incident reports, and compliance.
- Review of Security Technical Implementation Guidelines (STIGs).

Tools and Software:
- Metasploit
- Manage Engine Patch Manager
- Wireshark
- Ghidra
- Falcon CrowdStrike
- Kali Linux
- PowerShell
- Confluence
- BitLocker
- Confluence
- OWASP
- Windows Server Update Services
- Microsoft Azure Active Directory

Professional Development:
Actively engage in continuous learning and professional development within the cybersecurity field.

References:
Available upon request.