Imran Nawaz | Clifton, VA | Imran.nawaz@gmail.com | (703) 625-6873
https://www.linkedin.com/in/nawaz-imran
Top Secret Security Clearance

SUMMARY

Senior Governance, risk, and compliance (GRC) professional with 15+ years leading security compliance and risk programs across complex, cloud-first environments. Deep expertise with NIST 800-53, ISO 27001, FedRAMP, and CMMC. Known for building pragmatic control environments, simplifying audits, and driving down risk backlogs; while partnering with cross-division teams including engineering, product, legal and c-suite leadership.

CORE COMPETENCIES

- Project Management, Risk Management, Risk Assessment & Treatment; Control Design & Implementation; Audit/Assessment Readiness; Continuous Monitoring. Information security
- Risk Register tracking/Issue Management; Policy/Standards/Procedures; Third- Party Risk (Cloud/SaaS); Metrics/KRIs/KPIs & Executive Reporting
- Cloud Compliance (AWS/Azure); Vulnerability Management (Tenable/Nessus, WebInspect); ServiceNow GRC; Jira/Confluence
- Cross-functional collaborator, Agile, Communicator, Critical Thinker, Problem Solver

SELECTED ACCOMPLISHMENTS

- Implemented and maintained risk management frameworks across organizations to ensure compliance with regulatory requirements.
- Reduced open risk backlog by instituting corrective action SLAs and a weekly review, clearing 300+ risk register items, and cutting the average age of issues.
- Standardized control narratives and evidence requests across programs, decreasing audit prep time and rework.
- Automated and streamlined efforts via Agile project management to achieve system accreditation.

CERTIFICATIONS

CISSP • CISM • CISA • CRISC • PMP • CGRC • CCSK • CMMC RP • ISO/IEC 27001 Lead Implementer• ISO/IEC 42001 Lead Implementer • AIGP

TOOLS & TECHNOLOGIES

AWS • Azure • Tenable/Nessus • Cloud Technologies • ServiceNow GRC • Jira/Confluence • Microsoft 365

FRAMEWORKS & DOMAINS

NIST 800-53 • NIST RMF • NIST AI RMF • FedRAMP • CMMC (NIST 800-171) • ISO/IEC 27001 • ISO 42001• Privacy (PII/PHI) • SOC2 • PCI-DSS

EDUCATION

Western Governors University — B.S., Cybersecurity & Information Assurance — In Progress (June 2027)

Northern Virginia Community College — Business Information Technology Certificate — Jan 2023

PROFESSIONAL EXPERIENCE:

Sr. GRC Lead | 22nd Century Technologies LLC (US Army contract) | McLean, VA | July 2025 – Present

Sr. GRC SME | QBE LLC (US Army contract) | Haymarket, VA | Apr 2021 – July 2025

- Lead GRC/Certification initiatives across multiple AWS and Azure environments(IL-5/IL-6). Ensured controls meet NIST 800-53, FISMA, FedRAMP, and Army policy.
- Lead a team of Six ISSO's in securing ERP (War Fighter, Financial, HR) Army Cloud information systems.
- Stood up and run our third-party continuous monitoring program from onboarding and assessments to remediation and reporting.
- Managed customer and partner due diligence: answered security questions, pull policies/evidence, support audits, and explain our risk posture in plain English.
- Built a remediation plan that cleared 300+ items in the risk register by setting owners and deadlines and running weekly reviews and escalations.
- Performed third-party risk and FedRAMP CSO assessments before onboarding, track findings through closure with control owners and vendors.
- Reviewed, drafted, and maintained security policies and standards to comply with organizational and regulatory requirements.
- Improved how we work dashboards, metrics, and SLAs—to cut audit response time and boost control effectiveness.
- Partner closely with engineering, app, and infrastructure teams to prioritize and fix vulnerabilities, aligning remediation with delivery timelines.

Corporate Duties:

- Led a CMMC readiness gap analysis across people, process, and technology, identifying control deficiencies against CMMC requirements and prioritizing remediation efforts based on risk.
- Developed and presented a CMMC remediation roadmap with actionable recommendations, helping stakeholders strengthen security controls, documentation, and audit readiness.
- Kept ISO 27001:2013 documentation and evidence up to date for surveillance and recertification audits.

Security Engineer / Assessment & Authorization (A&A) Lead | ECS Tech / Tellenger (DHS) | Fairfax, VA | Apr 2017 – Apr 2021

- Led a GRC team on policy, certification, and enterprise risk assessments, turning gaps into actionable remediation plans aligned to NIST RMF.
- Built security into the CI/CD process—assessing deployment risk and enforcing policy across the SDLC so releases were safer without slowing the team down.
- Wrote and maintained policies, control standards, and procedures; prepared A&A/ATO artifacts; supported audits with clear, concise evidence.
- Drove remediation with infra/app/vendor teams and improved visibility with metrics, executive dashboards, and regular readouts.
- Strengthened compliance monitoring and reporting for critical systems, increasing control reliability and stakeholder confidence.
- Manage multiple compliance projects simultaneously

Sr. Information Systems Security Officer (ISSO) | Spry Methods (DOI) | McLean, VA | Jan 2017 – Apr 2017

- Drove Continuous Monitoring per NIST SP 800-37; performed targeted control assessments and risk analyses to prioritize fixes.
- Built relationships with business and engineering stakeholders; streamlined evidence collection and issue tracking.
- Proactively identified security risks and collaborated with partners as well as key stakeholders to monitor, reduce or eliminate risk.

Sr. Information Systems Security Officer (ISSO) | Rain IS Solutions (FCC) | Burke, VA | Sep 2016 – Jan 2017

- Executed Continuous Monitoring; validated scan results, removed false positives, and tracked remediation in CSAM (GRC tool).
- Participated in change review forums to assess security impact and ensure alignment with policy.

Information Systems Security Officer (ISSO) | Seidcon (USPTO) | Vista, CA | Jan 2014 – Sep 2016

- Led GRC activities supporting Continuous Monitoring and RMF; created governance documentation (policies, standards, control narratives).
- Managed centralized risk register; coordinated mitigation with owners across cloud and on Prem systems; reported status to leadership.
- Directed remediation that resolved 95% of known vulnerabilities across five business applications.

Information Systems Security Officer (ISSO) | NazIT Solutions (USDA) | Blacksburg, MD | Jan 2013 – Jan 2014

- Developed a Plan of Action and Milestones (POAM) remediation strategy to address the backlog of existing POAMs, enhancing risk mitigation efforts.
- Directed the management and remediation of open risks impacting government information systems through the robust utilization of the risk register.
- Maintained accurate and current records of all remediation activities, ensuring transparency and accountability in compliance efforts via the risk register.