Job Analysis: Senior Risk Management Framework

Derrick Amissah

OLD DOMION UNIVERSITY

IDS 493 Electronic Portfolio

Dr. Gordon-Phan

September 6, 2026

Abstract

Communication skills are also part of a successful career in cybersecurity. This paper will examine a Senior Risk Management Framework (RMF) Cyber Security Analyst position with Science Applications International Corporation (SAIC) for the Defense Counterintelligence and Security Agency (DCSA). The paper will detail the organization's purpose, key responsibilities of the position, and technical competencies needed. In addition, other competencies that might not be explicitly stated will be identified. Upon examination of the job description, it is apparent that compliance in cybersecurity involves interacting with a variety of individuals within the government technology (GovTech) community. Furthermore, cybersecurity training and coursework will be related to my experience as an IT help desk technician being exposed to identity and Access Management (IAM), security policies, technical troubleshooting, and other competencies. Finally, this paper will demonstrate that successful security authorization involves more than technical competencies. Other competencies such as communication, problem solving, and stakeholder adaptation to technical.

Cybersecurity has evolved from a back-end function to a business-critical function due to the increased sophistication of cyber threats in both the civilian and DoD sectors. Today, organizations require more than technical capabilities in their cybersecurity personnel. They require individuals who can effectively communicate between technical staff and business decision makers while also adhering to security principles. We can use job descriptions to gain insight into the expectations of employers regarding cybersecurity personnel.

An example is the Senior Risk Management Framework (RMF) Cyber Security Analyst position with Science Applications International Corporation (SAIC) located in Quantico, Virginia. This position works for the Defense Counterintelligence and Security Agency (DCSA) (SAIC, n.d.). This report will analyze the technical, interpersonal, and communication skills necessary for the position at SAIC. Specific skills mentioned within the job description as well as implied skills will be analyzed. Furthermore, ties will be made to study the required skills for the workforce and related personal education and employment experiences. The overall conclusion will be that technical skills including system accreditation, vulnerability scanning, NIST standards and the like are important, but also interpersonal, critical thinking, problem solving, adaptability and communication skills that can be acquired through college and IT experience are important as well. These skills allow for successful collaboration across organizational functions, ability to meet security standards, organizational support for critical information, systems and data, as well as problem solving.

SAIC is a defense and technology firm that provides engineering, mission support and IT services to government agencies including civilian, defense, space, intelligence and defense (SAIC, n.d.). This role contributes to the DCSA with their “One IT” initiative that aims at integrating and enhancing IT systems into a single secure environment. DCSA manages over

13,000 entities and facilities that deal with national security information. DCSA is also responsible for the security accreditation of systems within classified facilities. (SAIC, n.d.). These systems contain sensitive data. As a result, the Senior RMF Cyber Security Analyst is responsible for ensuring security and compliance with cybersecurity requirements within these systems. The analyst is also responsible for reviewing security controls and providing protection from potential security and cyber threats to critical defense information systems.

This position's primary role involves implementation and approval of systems within the Department of Defense (DoD) Risk Management Framework (RMF). The RMF consists of seven steps: preparation, categorization, selection of security controls, implementation, assessment, authorization, and continuous monitoring (SAIC, n.d.). Daily, the analyst ensures the maintenance of security documentation within eMASS, monitors vulnerability scans from tools including Nessus and Assured Compliance Assessment Solution (ACAS) and ensure that Plan of Action and Milestones (POA&M) items are resolved. Additional tasks include annual reviews of documentation, creation of System Security Plans (SSP), validation of risk assessments, and Information System Security Officer (ISSO) functions. All activities adhere to DoD 8500 and 8510 security policies (SAIC, n.d.).

The job qualifications list the technical skills that a qualified candidate should possess. The candidate is required to possess a Secret security clearance, a bachelor's in information technology, Cybersecurity, or a related discipline, and a minimum of five years of hands-on cybersecurity experience (SAIC, n.d.). Additionally, the position is seeking DoD 8570-M/8140-M IAT Level II credentials and experience with the Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs), NIST SP 800-53 security controls and Microsoft Office products. All these qualifications indicate that SAIC is seeking an

individual with strong knowledge in cybersecurity and practical experience with defense authorization and security tools.

In addition to the technical skills, there are also key interpersonal skills noted in the position that define the appropriate use of the technical capabilities. The position describes the analyst as someone who will link technical engineers to Information System Security Officers (ISSOs) to senior management; collaborate with Program and Project Managers; and recommend methods for risk reduction (SAIC, n.d.). All these qualifications imply that technical competency alone is not the end goal. The analyst is also expected to translate complex vulnerability data into understandable language and then link that data to business decisions that are useful to senior management.

There is evidence in studies that highlights the value of these soft skills. According to Henry (2019), approximately 67% of HR professionals would employ an individual with excellent soft skills who may lack all required technical capabilities. This is due to the ability to adapt to change in the workplace, through the skills of empathy, understanding, and listening which can be improved through time (Henry, 2019). Harris and Clayton (2018) have also found that technical competence and basic employment skills have become increasingly relevant due to the rapid change in technology. There is a shift towards valuing individuals who are adaptive to change, good at communication, and passionate about their work over those who only possess static technical competencies. These competencies allow an employee to be able to adapt to a changing workplace and across various roles (Harris & Clayton, 2018).

The job at SAIC, a role as a DCSA One IT analyst, has various roles beyond technical functions. These analysts have the ability to interact with engineers, adhere to security policies,

and interact with management. The analyst will ensure the availability of critical systems, perform problem resolution from ACAS scans and monitor POA&Ms. The analyst will also need to possess strong conflict resolution, negotiation, collaboration, and communication skills especially when dealing with security updates. Additionally, the analyst will be able to communicate security issues to management in a concise and understandable manner (SAIC, n.d.). Harris and Clayton (2018) suggest critical thinking allows an analyst to interpret data beyond the surface level. This skill is crucial to follow NIST directives, federal regulations, DISA STIGs, and RMF.

As a Cybersecurity student at ODU, I am exposed to vulnerabilities, risk, and security controls. I also obtain experience in security risks and policies. At the ODU IT Help Desk I gain hands on experience with IAM, MFA, troubleshooting, ServiceNow and more. I also gain experience with time management, patience, problem solving, communication, and more. I hope to use these experiences to eventually be able to work in technical groups, implement risk management, and be able to work with POA&M, ATO, RMF, and more.

In researching the Senior RMF Cyber Security Analyst position with SAIC, I have learned that successful cyber security involves both technical and people skills. Technical skills such as vulnerability scanning, STIGs, eMASS, RMF are important as well as people's skills such as critical thinking, adaptability, teamwork, and communication. My IT Help Desk experience and study of cyber security allows me to gain both types of skills and pursue a career in securing government assets

References

Harris, R., & Clayton, B. (2018). Editorial: The importance of skills – but which skills? *International Journal of Training Research*, 16(3), 195–199. https://doi.org/10.1080/14480220.2018.1576330

Henry, H. (2019). *Top soft skills in the 21st century workplace*. Junior Achievement of South Florida. https://jasouthflorida.org/top-soft-skills-in-the-21st-century-workplace/

SAIC. (n.d.). *RMF cyber security analyst senior* [Job posting]. ClearanceJobs. https://www.clearancejobs.com/jobs/9108801/rmf-cyber-security-analyst-senior?source=job_search