Aligning My Skills with the Security Engineering Associate Role at Goldman Sachs

Nehemia Araia

The University of Old Dominion

IDS 493: Electronic Portfolio Project

Dr. Phan

February 8, 2026

Abstract

Goldman Sachs is a global financial institution that treats cybersecurity and technology risk as core components of its business strategy rather than secondary concerns. The Security Engineering Associate position within the company's Technology Risk Advisory team is designed to assess cloud security risks, review secure architecture designs, embed security into software development processes, and provide technical guidance to engineers and stakeholders. The role blends technical analysis, risk evaluation, automation, and collaboration, reflecting Goldman Sachs' approach of integrating security deeply into its technology and business operations. The job advertisement emphasizes key skills such as cloud security assessment, scripting and automation, baseline cybersecurity knowledge, and clear technical communication, while also implying the importance of softer skills such as adaptability, collaboration, and time management. By analyzing the responsibilities, qualifications, and language of the job ad, this essay will demonstrate how my coursework in security, hands-on cloud projects, and internship experience in incident response have prepared me for this role. It also considers broader industry trends in cloud adoption and cybersecurity that drive demand for positions like this. Ultimately, the analysis shows that my technical foundation, problem-solving mindset, and interests align closely with Goldman Sachs' expectations for a Security Engineering Associate.

Cybersecurity has become inseparable from modern finance, and Goldman Sachs' job advertisement for a Security Engineering Associate reflects this reality. Rather than treating security as a reactive function, the company frames it as an integrated, strategic discipline that shapes how technology is built and operated. The job description does more than list technical tasks; it reveals how Goldman Sachs views risk, innovation, and collaboration within its Technology Risk organization. My thesis is that the structure, language, and priorities of the Security Engineering Associate role align strongly with my academic and technical skills, and professional experiences, which position me as a strong fit for this role while also picturing how this position supports Goldman Sachs' broader mission of securing its digital ecosystem.

The overall role of this position is to serve as both a technical assessor and an advisory partner within Goldman Sachs' Technology Risk organization. The ad explains that the Technology Risk team is "responsible for detecting and preventing attempted cyber intrusions against the firm, helping the firm develop more secure applications and infrastructure, developing software in support of our efforts, measuring cybersecurity risk, and designing and driving implementation of cybersecurity controls." This framing suggests that the role is not limited to monitoring threats but actively shapes how security is embedded into technology. The position sits specifically within the Technology Risk Advisory team, described as "the consultative and technology subject matter expertise arm," which indicates that the role requires analytical judgment, communication, and influence, not just technical execution. The title "Security Engineering Associate" does not include a senior ranking such as "I" or "II," which suggests it is intended for recently graduated professionals who bring foundational knowledge rather than extensive years of industry experience. However, the responsibilities, such as conducting "comprehensive cloud security assessments" and performing "software architecture

design reviews," imply that even at the Associate level, Goldman Sachs expects a high level of technical skills and professionalism

The selection criteria in the Qualifications section reveal which skills Goldman Sachs prioritizes and how the organization structures its expectations. The first requirement listed is "Development / Scripting / Coding Skills," specifically calling out proficiency in Python, PowerShell, or Bash for "automation, data analysis, or security tooling." Placing this at the top signals that automation and technical problem-solving are central to the role rather than optional. The next requirement, "Baseline Security Knowledge," emphasizes familiarity with core cybersecurity domains such as network security, identity and access management, and vulnerability management, suggesting that the firm expects candidates to think holistically about security rather than in silos. The ad also highlights "Cloud Fundamentals," requiring a "foundational grasp of cloud computing concepts and architectures" and "prior project experience in cloud," which aligns with Goldman Sachs' stated focus on building "native public cloud applications." The organization of these qualifications, moving from technical skills to analytical thinking and finally to communication, suggests that while technical ability is essential, Goldman Sachs equally values critical thinking and the ability to "articulate technical concepts to both technical and non-technical audiences."

Considering the duties of the position, several additional unstated skills would likely be valuable for success in this role. Because the job requires frequent collaboration with engineering and development teams, strong interpersonal skills and emotional intelligence would be important for navigating differing perspectives and building trust. The responsibility to "stay updated on emerging cloud security threats, technologies, and regulatory requirements" implies that self-motivation, curiosity, and continuous learning are necessary traits in a fast evolving

field. Additionally, because the role involves documenting security controls and guardrails, strong technical writing skills and attention to detail would be critical to ensure clarity, consistency, and accountability. While these skills are not explicitly listed, they are implied by the nature of the work and the level of responsibility described in the ad.

The context of the job and the company highlights several important current and future motivators driving demand for this position. The financial sector is one of the most heavily targeted industries for cyberattacks, making robust security practices essential for protecting sensitive data and maintaining client trust. The job description explicitly references Goldman Sachs' "transition to building native public cloud applications," reflecting a broader industry shift toward cloud computing. As financial institutions increasingly migrate to cloud environments, the need for professionals who can assess cloud risks, design secure architectures, and implement automated security controls continues to grow. Additionally, evolving regulatory requirements around data protection, cybersecurity risk management, and operational resilience further increase the importance of roles like this. Goldman Sachs' description of its Technology Risk team as "one of the most progressive" in the industry suggests that the firm is investing heavily in cybersecurity innovation, making this position both relevant and future-proof in a rapidly changing landscape.

My reasons for wanting this position are closely tied to both my interests and my background. The job ad includes key terms such as "cloud security assessments," "secure architecture design patterns," and "CI/CD pipelines," all of which connect directly to courses and projects I have completed. In my cloud security coursework, I studied concepts like identity and access management, encryption, and secure network design, which are directly relevant to evaluating cloud environments. Through hands-on AWS projects, I have experience designing

secure architectures, implementing security controls, and automating compliance checks, which aligns with the responsibility to "develop and maintain scripts and automated solutions to streamline security processes." I am particularly drawn to the advisory aspect of the role because I enjoy analyzing risks and finding security solutions that balance protection with business needs. This role aligns with my strengths in incident response, threat analysis, and cloud security, while also allowing me to grow in areas like secure architecture design and enterprise risk assessment.

Goldman Sachs' culture, as reflected in the job ad, appears to prioritize collaboration, innovation, and proactive risk management. The description of the Technology Risk team as working "deeper into the organization" suggests a culture that values integration rather than isolation of security functions. The emphasis on partnering with engineers, guiding technology innovation, and embedding security into the SDLC indicates that teamwork, communication, and influence are highly valued. Additionally, the firm's focus on continuously improving its security posture and staying ahead of emerging threats suggests a culture of learning and adaptability. To fit well within this environment, a candidate would need to be not only technically skilled but also open-minded, collaborative, and willing to engage with diverse stakeholders. My experience working in team-based security projects and internships has helped me develop these qualities, making me a strong cultural fit for Goldman Sachs.

Reading between the lines of the ad reveals that time management is a crucial soft skill for this role, even though it is not explicitly stated. The responsibilities include conducting assessments, reviewing architectures, developing security controls, maintaining automation scripts, and contributing to incident response, all of which suggest a high workload with competing priorities. The requirement to "embed security best practices throughout the software development lifecycle (SDLC) and CI/CD pipelines" implies that security engineers must

operate within fast-paced development environments where delays could impact project timelines. This makes the ability to prioritize tasks, manage time effectively, and balance multiple responsibilities essential for success in the role.

The challenges associated with this position likely include balancing security requirements with business objectives, keeping up with rapidly evolving cloud technologies, and responding to high-pressure security incidents. However, the wording of the ad is generally encouraging and empowering rather than intimidating. Phrases such as “guiding technology innovation in terms of security and control” suggest that security is viewed as a strategic enabler rather than a barrier. The emphasis on collaboration and advisory responsibilities makes the role feel dynamic and impactful rather than purely reactive. Overall, the presentation of the ad makes me feel motivated and excited about the possibility of working at Goldman Sachs, as it portrays security as a respected and integral function within the organization.

In conclusion, the Security Engineering Associate role at Goldman Sachs represents a strong alignment between my skills, experiences, and career aspirations. The job requires a solid foundation in cloud security, scripting, and risk analysis, all of which I have developed through my coursework and hands-on projects. The emphasis on collaboration, advisory work, and continuous learning aligns with both my professional strengths and my personal values. By analyzing the responsibilities, qualifications, and underlying expectations of the job advertisement, it is clear that my background has prepared me to contribute meaningfully to Goldman Sachs’ Technology Risk team. As cybersecurity continues to play an increasingly critical role in the financial sector, I am eager to apply my skills in a high-impact environment that prioritizes innovation, security, and responsible technology development.

References

Goldman Sachs. (n.d.). *Security engineering associate*. Goldman Sachs Careers. https://higher.gs.com/roles/166206