"The Nation's Bank", **National Bank of Pakistan** aims to support the financial well-being of the Nation along with enabling sustainable growth and inclusive development through its wide local and international network of branches. Being one of the leading and largest banks of Pakistan, National Bank of Pakistan is contributing significantly towards socioeconomic growth in the country with an objective to transform the institution into a future-fit, agile and sustainable Bank.

In line with our strategy, the Bank is looking for talented, dedicated and experienced professional(s) for the following position in the area of **Risk Management.**

The individuals who fulfill the below basic-eligibility criteria may apply for the following position:

01	**Position / Job Title**	**Officer IS Applications / Cloud Security (OG-I)**
	Reporting to	Unit Head - IS Digital Channels
	Educational / Professional Qualification	• Minimum Graduation in Computer Science and / or Computer Engineering and / or Cybersecurity and / or Information Technology from a local or international university / college / institute recognized by the HEC of Pakistan • Candidates having relevant professional certifications in Information Security / Cybersecurity, such as CompTIA Security+, Comp TIA Cloud +, cloud & application security certifications will be preferred
	Experience	• Minimum 04 years of experience in Application Security and / or Cloud security and / or Information Security
	Other Skills / Expertise / Knowledge Required	• Good knowledge of Information Security function • Sound interpersonal, analytical and problem solving skills • Team player with ability to prioritize and meet strict deadlines • Knowledge of security principles, threat analysis and risk management
	Outline of Main Duties / Responsibilities	• To perform security reviews of web applications, mobile applications, APIs, databases, middleware, SaaS solutions and cloud hosted workloads • To conduct security assessments during solution design, implementation, major changes and production deployment • To review application architecture and identify security risks relating to authentication, authorization, session management, encryption, data handling, API's and integrations • To review applications against OWASP Top 10', OWASP API Security Top 10, secure coding standards and other security requirements • To review SAST, DAST, SCA and penetration testing findings and validate remediation and risk closure • To access third-party and internally developed applications for security weaknesses before production deployment • To perform or coordinate threat modeling for critical applications and significant technology changes • To review cloud architectures and configurations across AWS, Microsoft Azure and / or Google Cloud Platform • To assess cloud controls covering IAM, privileged access, network segmentation, security groups / firewalls, storage, databases, encryption, key management, secrets management, logging, monitoring, backup and recovery • To review cloud environments against relevant security baselines such as CIS Benchmarks and organizational cloud-security standards • To assess risks associated with IaaS, PaaS, SaaS, containers, Kubernetes, serverless computing and cloud native services

		• To review CI / CD pipelines and DevSecOps controls, including source code security, secrets handling, dependency management, container / image scanning and deployment controls • To evaluate IAM controls based on least privilege, segregation of duties, MFA, privileged access management and Zero Trust principles • To review API security, including authentication, authorization, rate limiting, encryption, token management and exposure of sensitive information • To review Infrastructure-as-Code (laC) templates and automated cloud deployments for security misconfigurations • To assess security implications of application and cloud changes through change management process • To maintain security review findings, risk ratings, remediation plans, exceptions and closure evidence • To work with application owners, developers, DevOps and cloud teams to recommend practical remediation measures • To participate in application / cloud related security incidents and provide technical support for investigation and root cause analysis • To develop and maintain application security standards, cloud security baselines, review checklists and security architecture requirements • To perform any other assignment as assigned by the supervisor(s)
	Place of Posting	Karachi

Assessment Test / Interview(s)	Only shortlisted candidates strictly meeting the above-mentioned basic eligibility criteria will be invited for test and / or panel interview(s).
Employment Type	The employment will be on contractual basis for three years which may be renewed on discretion of the Management. Selected candidates will be offered compensation package and other benefits as per Bank's Policy / rules.

Interested candidates may visit the website **www.sidathyder.com.pk/careers** and apply online within 10 working days from the date of publication of this advertisement as per given instructions.

Applications received after due date will not be considered in any case. No TA / DA will be admissible for test / interview.

National Bank of Pakistan is an equal opportunity employer and welcomes applications from all qualified individuals, regardless of gender, religion, or disability.