**GOVERNMENT OF PAKISTAN**
**NATIONAL DATABASE & REGISTRATION AUTHORITY**
**(Headquarters, G-5/2 Islamabad)**

# We Are Hiring

NADRA is seeking highly skilled and experienced professionals for the following positions:-

| Position & Age | Educational Background | Responsibilities, Skills and Experience Requirements |
|---|---|---|
| **Deputy Director (Governance, Risk Assessment & Compliance)**<br>*Age Max : 44 years* | • Bachelors (4 Years) in Computer Science/ Information Technology/Cyber Security<br>• Masters in Information/Cyber Security will be preferred<br>• Degrees must be recognized and attested by HEC | **Professional Experience**<br>• Preferably 6-8 years post-graduation experience, with at least 3 years in Governance, Risk Management, and Compliance roles<br>• Certification in ISO-27001, CISA and CGEIT will be preferred<br>**Skills and Competencies**<br>• Understanding of security frameworks, such as ISO 27001, PCI DSS, NIST SP and CIS Controls<br>• In-depth knowledge of technological advancements in Information Security and industry best practices<br>• Understanding of threat landscapes, vulnerabilities, and attack vectors<br>• Proficiency in risk assessment methodologies, risk identification, risk analysis, risk mitigation strategies, IS Policy formulation, writing of SOP's and instructions<br>• Proficiency in conducting Audit as per ISO requirements and formulation of Information Security Audit Reports<br>• Excellent communication skills, both written and verbal, for conveying information regarding security and compliance to various stakeholders<br>• Strong analytical skills to assess complex information security risks, evaluate compliance gaps, and develop effective solutions<br>• Experience to manage the SIEM, incidents knowledge base<br>• Experience to generate the daily, weekly and monthly reports<br>• Manage the assessment of web applications, mobile applications, APIs and review technical reports/ recommendations<br>• Collaborate with infrastructure teams to integrate security into the software development lifecycle (SDLC)<br>• Stay up to date on DevSecOps best practices and industry trends |
| **Deputy Director (Vulnerability Assessment and Penetration Testing - VAPT)**<br>*Age Max: 44 years* | • Bachelors (4 Years) in Computer Science/ Information Technology/Cyber Security/Information Security<br>• Masters in Information/Cyber Security or equivalent will be preferred<br>• Degrees must be recognized and attested by HEC | **Professional Experience**<br>• Preferably 6-8 years post qualification experience in Application/ Network Security and Penetration testing.<br>• CEH Certified, CHFI Certified preferable<br>**Skills and Competencies**<br>• Work closely with application development teams to provide security expertise on system, encryption, authentication, security specific code<br>• Knowledge of the following application technologies and standards (not limited to but including): HTML, CSS, JavaScript, SQL, JSON, Python, XML, SSL/TLS, REST, SAML, OAuth, C#, PHP is preferred, IAM<br>• Hands On Experience in Desktop, Web and Mobile Application Penetration Testing<br>• Expertise in deploying and operating security tools Metasploit, Burp Suite, Nessus, Kali Linux, Hydra, Dnspy, Mobsf, Mobile application security testing tools etc.<br>• Knowledge of software and network architecture and application security/pen testing standards like OWASP, SANS |

| | | |
|---|---|---|
| | | etc.<br>• Manage the assessment of web applications, mobile applications, APIs and review technical reports/recommendations<br>• Conduct source code reviews, static and dynamic application security testing (SAST, DAST)<br>• Knowledge of Cloud Security, Security Orchestration Platforms, Cluster, Containerization and DevSecOps. Able to develop and maintain code review guidelines and standards<br>• Collaborate with development teams to improve and provide recommendations on code quality and secure coding<br>• Collaborate with infrastructure teams to integrate security into the software development lifecycle (SDLC)<br>• Stay updated on programming languages and secure coding techniques<br>• Develop and maintain tools and scripts for automated security testing |
| **Assistant Director (Database Security)**<br>*Age Max : 37 years* | • Bachelors (4 Years) in Computer Science/ Information Technology/Cyber Security/Information Security or equivalent<br>• Degrees must be recognized and attested by HEC | **Professional Experience**<br>• Preferably 3 years technical hands-on experience in Database Security and Database Analytics<br>**Skills and Competencies**<br>• Installation, configuration and setup Guardium appliances for database activity monitoring and protection<br>• Installation of Guardium agents on database servers with necessary configurations for collection of logs<br>• Timely patching of Guardium appliances and renewal of license<br>• Monitor and evaluate database incidents through IBM Guardium data monitoring and protection tool<br>• Perform data discovery and classification with all stakeholders in order to prioritize implementation of security solution<br>• Request assistance from application owners to identify sensitive objects in their respective databases<br>• Monitor and audit all database activity including privileged user activity<br>• Monitor and analyze all database risks by performing data analytics of existing logs<br>• Securely store the audit logs to a central server outside the audited database<br>• Automate database incident reports and ensure incidents are handled by concerned departments in timely manner<br>• Expertise and knowledge in data analytics, as well as automate reporting on daily and weekly incidents. Resolution of incidents with data owners<br>• Enforce separation of duties by monitoring and logging database administrator activities<br>• Monitor user behavior and identify risks through active threat analytics |
| **Assistant Director (Governance, Risk Assessment & Compliance)**<br>*Age Max : 37 years* | • Bachelors (4 Years) in Computer Science/Information Technology/Cyber Security/Information Security/Computer Science or equivalent<br>• Degrees must be recognized and attested by HEC | **Professional Experience**<br>• Preferably 3 years post-graduation experience, with at least 2 years in Governance, Risk Management, and Compliance roles<br>• Certification in ISO-27001, CISA and CGEIT will be preferred<br>**Skills and Competencies**<br>• Solid understanding of different security frameworks, such as ISO 27001, NIST and CIS Controls<br>• Staying current on best practices and technological advancements and acts as a technical resource for security assessment and compliance |

| | | |
|---|---|---|
| | | • Performing other related duties as assigned from time to time based on the business requirements<br>• Deep knowledge of information security principles, practices, and technologies, including understanding of threat landscapes, vulnerabilities, and attack vectors<br>• Proficiency in risk assessment methodologies, risk identification, risk analysis, and risk mitigation strategies<br>• Proficiency in IS Policy formulation, writing of SOP's and instructions<br>• Proficiency in conducting Audit as per ISO requirements and formulation of audit reports<br>• Excellent communication skills, both written and verbal are important for conveying information security and compliance information to various stakeholders, including senior management and technical teams<br>• Strong analytical skills to assess complex information security risks, evaluate compliance gaps, and develop effective solutions |
| **Assistant Director (Cyber Threat Intelligence)**<br>*Age Max : 37 years* | • Bachelors (4 Years) in Computer Science/ Information Technology/Cyber Security/Information Security/Computer Science or equivalent<br>• Degrees must be recognized and attested by HEC | **Professional Experience**<br>• Preferably 3 years post-graduation experience, with at least 1 year in Cyber Threat Intelligence (CTI), Threat Hunting, or Incident Response roles<br>• Certification in EC Council (CTIA) will be preferred<br>**Skills and Competencies**<br>• Hands-on experience with Threat Intelligence platforms, YARA rules, Sigma rules, and OSINT tools<br>• Familiarity with MITRE ATT&CK framework, dark web monitoring, and threat actor tracking<br>• Knowledge of IOC (Indicators of Compromise) gathering, analysis, and sharing with relevant stakeholders<br>• Continuously monitor dark web, Telegram, Discord, Twitter, and threat intelligence platforms for potential threats targeting the organization<br>• Identify, validate, and enrich IOCs (IPs, hashes, domains, etc.) for integration into security controls like SIEM, EDR, and Firewalls<br>• Maintain and enhance threat intelligence tools and platforms for better detection and analysis<br>• Issue timely advisories and alerts on emerging threats, vulnerabilities, and exploits, and escalate incidents when necessary<br>• Stay updated on new security technologies, AI-driven cyber threats, and advanced attack techniques |

**Job Location:** Islamabad

**Terms & Conditions**

1. Selected candidate will be hired initially for contract period of 5 years (extendable if required).
2. Management reserves the right to accept/reject any application without assigning any reason.
3. Only shortlisted candidates will be called for test/interview.
4. Candidate shall be disqualified if false information is provided.
5. Employees serving in Government/Semi-Government departments must provide/attach No Objection Certificate (NOC) at the time of submission of application.
6. 5 years' relaxation in age is already included in above age limit.
7. Selected candidate shall provide Medical Fitness and Character Certificates.
8. No TA/DA will be admissible.
9. Attested degrees from Higher Education Commission (HEC)/ relevant regulatory bodies must be provided at the time of interview.
10. Females, Minority, Transgenders and Differently-abled candidates are encouraged to apply.

11. Electronic gadgets, mobile phones, smart watches etc. will not be allowed during test and interview.
12. The deadline for submission of application is **2nd March, 2025**
13. For further details and to apply, please visit **https://careers.nadra.gov.pk**

**HR Directorate**
**National Database & Registration Authority**
**State Bank of Pakistan, Shahrah-e-Jamhuriat, Sector G-5/2, Islamabad**