10.Post:	**Project Associate (Information Security Audit)**
Position Code:	PA(ISA)
No. of Posts	02
Location	C-DAC, Silchar
Duration of the position	Three Years
Minimum Educational Qualification	B.E/ B. Tech or equivalent degree in Computer Science/Information Technology/Electronics OR Post Graduate Degree in Computer Science/Masters in Computer Application OR M.E/M.Tech or equivalent degree in CSE/IT/Electronics
Minimum Post Qualification Relevant Experience	NIL
Desirable Skills (in one or more topics)	• Knowledge of basic network concepts such as TCP/IP protocol stack. • Knowledge of security protocols such as IPSec, VPN, SSL, TLS, SNMPv3, etc. • Knowledge of cryptography and cryptographic algorithms. • Knowledge of security standards like ISO 27001, PCI DSS, cyber security laws. • Knowledge of perimeter security solutions like firewall, IDS, IPS, UTM, WAFs and security analysis tools. • Knowledge of Python. • Knowledge of E-mail frauds analysis. • Knowledge of Network Management and Monitoring tools. • Experience in vulnerability assessment and penetration testing of web applications, operating systems, network equipment, wireless, mobile phones & databases. • Familiar & hands-on experience with commercial/open-source VAPT tools such as NMAP, Nessus, OWASP Zap, Burp suite, Netsparker, and exploit frameworks like Metasploit. • Proficiency in dedicated Linux distributions like Kali Linux, Parrot OS, and packet analysis tools like Wireshark. • Experience and proficiency in Ethical Hacking. Preferred – • Prior Job experience in relevant field is preferred. • Candidates having SANS certifications or CEH
Job Profile and other Skills	• Perform vulnerability and penetration testing of network infrastructure, servers, websites, and databases. • Test compliance for various cybersecurity standards towards implementation of security policies and controls. • Implement and mainlining security controls by adopting International best practices. • Internet traffic monitoring. • IP, Domain Name, user profiles tracking using Open Source Intelligence.

	• Carry out proactive security testing based on the defined policies and control structures as a routine activity. • Conduct and ensure periodic infrastructure audits (network, servers, and systems) and investigation of any cyber violations • Analyze and assess the infrastructure's vulnerabilities (software, hardware, networks) and devise possible countermeasures. • To be part of the Blue team and red team cyber security drills. • Ensure business continuity with effective backup and disaster recovery plans and procedures. • Ensure cyber security practices and secure SLDC for all in-house and outsourced applications development. • Implement system security engineering across the program acquisition life cycle performing and analyzing a range of IA/ C&A assessment activities. • Responsible for developing the design process and security policies and updating the gaps in the Information Security practices to the Senior management.
Mode of selection	Written Test cum Interview
Emoluments	Consolidated pay : **Rs.25,000-35,000 p.m** At present the salary and other benefits include Consolidated pay, Medical Reimbursement, Provident fund, Food / Canteen Subsidy, Leave Encashment, Gratuity and annual increment (as per the performance).