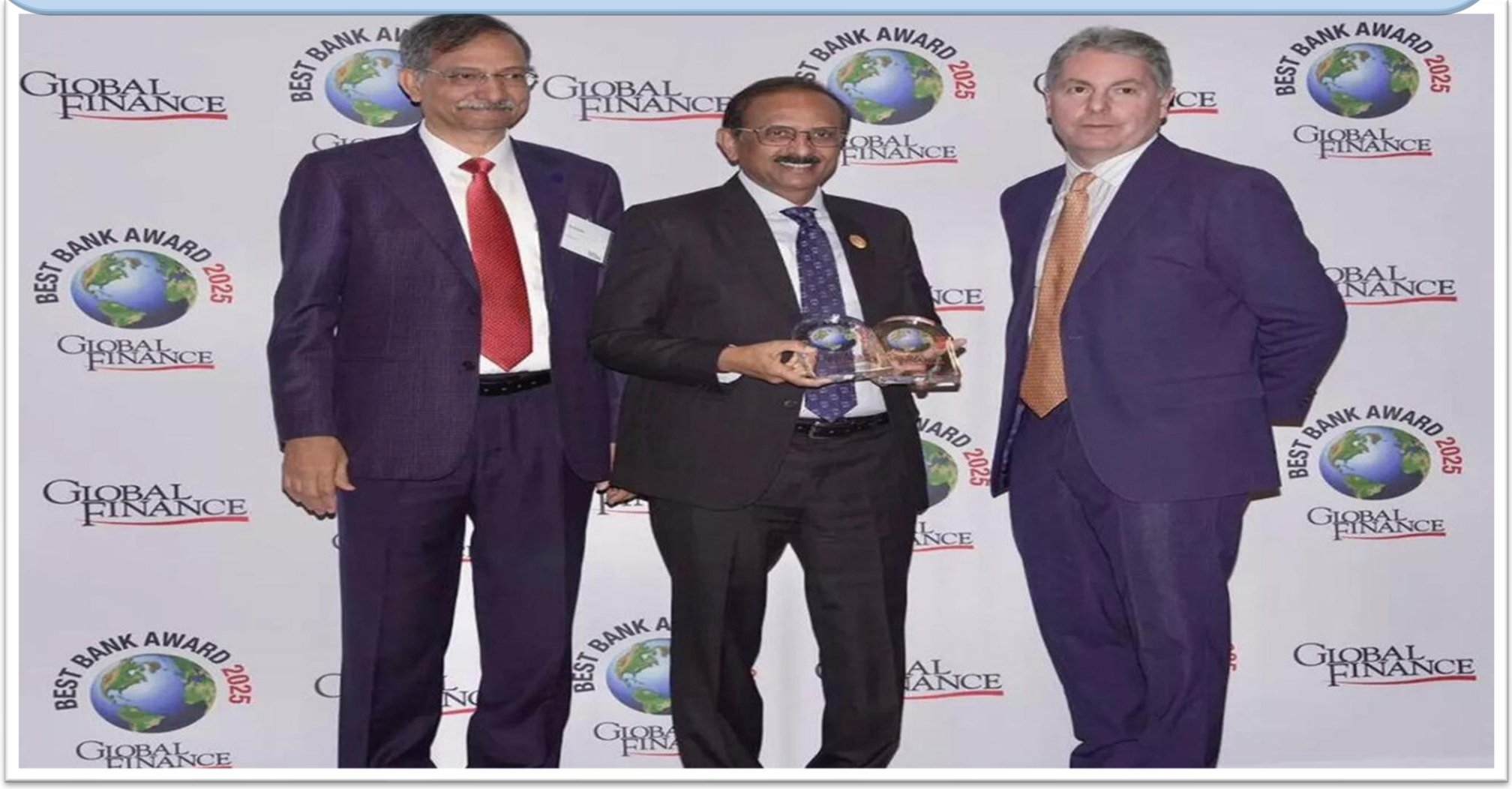
State Bank of India

Central Recruitment & Promotion Department
Corporate Centre, Mumbai
Email: crpd@sbi.co.in

SBI RECOGNISED AS “WORLD’S BEST CONSUMER BANK-2025 AND “BEST BANK IN INDIA-2025” BY GLOBAL FINANCE



RECRUITMENT OF SPECIALIST CADRE OFFICERS ON REGULAR BASIS
(ADVERTISEMENT NO: CRPD/SCO/2025-26/25)
ONLINE REGISTRATION OF APPLICATION & PAYMENT OF FEES: FROM 24.02.2026 TO 16.03.2026

State Bank of India invites online applications from eligible Indian citizens for appointment to the Specialist Cadre Officers Posts on Regular Basis. Candidates are requested to apply online through the link given on Bank's official website https://sbi.bank.in/web/careers/current-openings. The candidates, who intend to apply for the Post(s) are advised to apply only after carefully reading and understanding the undernoted contents of this notification.

IMPORTANT INSTRUCTIONS:

1.	Before applying, candidates are requested to ensure that they fulfil the eligibility criteria for the post(s), as on the date of eligibility. Candidates are required to apply online through the website **https://sbi.bank.in/web/careers/current-openings** The process of Registration is completed only when fee is deposited with the Bank through online mode on or before the last date for payment of fee.
2.	Candidates are required to apply for the post(s) online through the link given on Bank's official website only and no other mode of application will be entertained. Hard copy of application & other documents need not to be sent to this office. Candidates are advised in their own interest to apply online well before the closing date and not to wait till the last date to avoid the possibility of disconnection / inability/ failure to log on to the website on account of heavy load on internet or website jam. SBI does not assume any responsibility for the candidates not being able to submit their applications within the last date on account of aforesaid reasons or for any other reason beyond the control of SBI.
3.	Before submission of the application, candidates must check that they have filled in correct details in each respective field of the application form. After expiry of window for online application, no change/correction/modification will be allowed under any circumstances. Requests received in this regard in any form like Post, Email, by hand etc. shall not be entertained and will be summarily rejected.
4.	Candidates must have valid Email ID and Mobile phone number which should be kept active till the declaration of result and issuance of call letters on final selection, if any. It will help him/her in getting call letter/Interview advice etc. by email or over mobile by SMS.
5.	The Bank reserves the right to post / transfer the recruited / engaged officers to any of the offices of State Bank of India, in India or to depute to any of the associates / subsidiaries or any other organization depending upon the exigencies of the services. Request for posting / transfer to specific circle/place / office may not be entertained.
6.	Candidates are advised to check Bank's website **https://sbi.bank.in/web/careers/current-openings** regularly for details and updates. **No separate intimation will be issued in case of any change / update. All Changes/ Updates/ revisions / Corrigendum / results / schedules / list of shortlisted / selected candidates etc. will be hosted only on Bank's website only.** The Call letter/ advice, wherever required, will be sent by e-mail only **(No hard copy will be sent**).
7.	Candidates are required to upload all required documents (Resume, ID proof, Age proof, Caste Certificate (if applicable), PwBD Certificate (if applicable), Educational qualification, other qualifications/ certifications, Proof of Experience etc.) failing which their application / candidature will not be considered for Shortlisting / Interview.
8.	The Candidates applying for the post should ensure that their admission to all the stages of the recruitment (e.g. shortlisting, interview etc.) will be purely provisional subject to satisfying the prescribed eligibility conditions. Short listing will be provisional without verification of documents. Candidature will be subject to verification of all details/ documents with the original when a candidate reports for interview (if called).
9.	The selected candidates may be offered appointment in the bank subject to their completing other formalities such as verification of eligibility, credentials, certificates, satisfactory reports from the references, medical examination and verification of antecedents etc.
10.	Candidate(s) seeking age relaxation, fee exemption must submit valid requisite certificate of the Competent Authority in the prescribed format, when such certificate is sought at the time of document verification. Otherwise, their claim will not be entertained, and their candidature will be liable for cancellation / rejection.
11.	Candidates against whom there is/ are adverse report regarding character & antecedents, moral turpitude are not eligible to apply for the post. If any such adverse orders / reports against the shortlisted/ selected candidates is found/ received by the Bank post their selection, their candidature/ services will be rejected forthwith.
12.	**Candidates are not allowed to apply for more than two posts.**
13.	In case more than one application (multiple applications) are submitted by a candidate for the **same post**, only the last valid (completed) application will be retained, and the application fee, if any, paid for the other registrations will stand forfeited. Further, multiple attendance/ appearance by a candidate at the time of interview / joining will result in rejection/ cancellation of candidature, summarily.

14.	**In case a candidate applies for more than two posts, only the last valid (completed) application for two different posts will be retained, and the application fee, if any, paid for the other registrations will stand forfeited.**
15.	The Bank reserves the right to change the notified vacancies including the reserved vacancies without assigning any reason(s), whatsoever.
16.	The Bank reserves the right to cancel / modify the recruitment process entirely or partially at any stage / time for any particular post / all the posts, if so warranted, without assigning any reason thereof and the Bank shall not be liable to refund the fee or pay any compensation to the applicant.
17.	Candidates furnishing false information / suppressing the facts will be disqualified and shall be liable for debarment and legal/criminal action. Candidates who attempt fraud/impersonation shall be liable to be debarred from future recruitment process conducted by the Bank.
18.	The selected candidates, after appointment, shall be on probation as per Bank's extant recruitment Policy in force / amended/ modified from time to time, for the respective Post(s).
19.	All appointments under this project shall be entirely at the discretion of the Bank and shall be made at the starting stage of the pay scale admissible to the post.
20.	The Bank will decide the Venues(s) / Centre(s) for interview, if shortlisted. Candidates will have to appear for the interview, if called, at a center / venue as decided by the Bank and no request in this regard will be entertained by the Bank.
21.	In case a candidate is called for interview and is found not satisfying the eligibility criteria (Age, Educational Qualification, Other qualification, Experience etc.) he/ she will neither be allowed to appear for the interview nor be entitled for reimbursement of any travelling expenses.
22.	In case more than one candidate score same marks as cut-off marks in the final merit list (common marks at cut-off point), such candidates will be ranked in the merit according to their age in descending order.
23.	The Bank takes no responsibility for any delay in receipt or loss of any communication, whatsoever.
24.	Candidates serving in Govt./ Quasi Govt. offices, Public Sector undertakings including Nationalized Banks and Financial Institutions are advised to submit **'No Objection Certificate' from their employer at the time of interview, failing which their candidature will not be considered** and travelling expenses, if any, otherwise admissible, will not be paid.
25.	In case of selection, candidates will be required to produce proper discharge certificate from the current employer at the time of taking up the appointment.
26.	**CIBIL**: **Candidates who have defaulted in repayment under any lending arrangement with Banks / NBFCs/ Financial Institutions including credit card dues and have not regularized / repaid their outstanding thereunder till the date of issuance of letter of offer of appointment by the Bank, shall not be eligible for appointment to the post. However, candidates who have regularized / repaid such outstanding on or before the date of issuance of offer of engagement/appointment, but whose CIBIL status has not been updated on or before the date of joining, shall have to either get the CIBIL status updated or produce the NOCs from lender to the effect that there is no outstanding with respect to the accounts adversely reflected in the CIBIL, failing which the letter of offer shall be withdrawn / cancelled. Thus, the candidates with record of default in repayment of loans/ credit card dues and/ or against whose name adverse report of CIBIL or other external agencies are available are not eligible for engagement/appointment.**

A. DETAILS OF POSTS/ NATURE OF ENGAGEMENT /GRADE / VACANCY/ AGE:

Sl. No.	Name & Type of Post	Nature of Engagement/Grade	Vacancies			PwBD #	Age in years^ (As on 31.12.2025)	
			UR	OBC	Total	VI	Min	Max
1.	Deputy Manager- IT Security Expert	**Regular (MMGS-II)**	**1**	**--**	**1**	--	25	35
2.	Deputy Manager -Emerging Technology		3	**1**	4	1		
3.	Deputy Manager -Cyber Security Analyst		2	**--**	2	1		
4.	Deputy Manager -Incident Management & Forensics		2	**--**	2	1		
5.	Deputy Manager -Test Engineers		3	**--**	3	1		
	Total		**11**	**1**	**12**	**4**		

- Horizontal vacancy
^ Age relaxation is available as per Government of India guidelines.

ABBREVIATIONS: **UR –** Unreserved, **PwBD** - Persons with Benchmark Disabilities, **OBC**-Other Backward Classes, **VI**- Visually Impaired.

IMPORTANT POINTS:

1. Reservation for PwBD candidates is horizontal and is included in the overall vacancy of the respective parent category (wherever applicable).
2. The number of vacancies including reserved vacancies mentioned above are **provisional and may vary** according to the actual requirement of the Bank.
3. Posting / Placement / Utilization of the selected candidates will be done at the sole discretion of the Bank.
4. Maximum age indicated is for Unreserved category candidates. **Relaxation in upper age limit** will be available to reserved category candidates as per Govt. of India guidelines (wherever applicable).
5. The reservation under various categories will be as per Government of India Guidelines (wherever applicable).
6. Candidate belonging to OBC category but coming in the 'Creamy Layer' are not entitled to OBC reservation and age relaxation. They should indicate their category as 'UR' or UR (PwBD) as applicable.
7. A declaration will have to be submitted in the prescribed format by candidates seeking reservation under OBC category stating that he/she does not belong to the creamy layer as on last date of online registration of application. **OBC certificate containing the 'non-creamy layer' clause, issued during the period 01.04.2025 to the date of interview, should be submitted by such candidates, if called for interview**. No request for extension of time for production of requisite certificate beyond the said date shall be entertained and candidature will be cancelled.
8. Candidates belonging to reserved category including Person with Benchmark Disabilities (PwBD) for whom no reservation has been mentioned are free to apply for vacancies announced for Unreserved category provided they fulfil all the eligibility criteria applicable to Unreserved Category.
9. Benefit of reservation/ relaxation (**if any**) under reserved category (i.e. SC, ST, OBC) including PwBD category can be availed of only upon production of valid Caste certificate issued by the Competent Authority on format **prescribed by the Government of India.**
10. Relaxation in Upper age limit shall be as below (**wherever applicable**):

Sl.	Category		Age relaxation (In years)
a)	Other Backward Classes (OBC) (Non-Creamy Layer)		3
b)	Scheduled Castes/ Scheduled Tribes (SC/ ST)		5
c)	Persons with Benchmark Disabilities (PwBD)	- PwBD (UR/ EWS)	10
		- PwBD (OBC)	13
		- PwBD (SC/ ST)	15

NOTE: Cumulative age relaxation will not be available either under the above items or in combination with any other items. Candidates seeking age relaxation are required to submit copies of necessary certificate(s) at the time of interview, if shortlisted. No change in the category of any candidate is permitted after registration of online application, no correspondence/email/phone will be entertained in this regard.

11. PwBD candidate should produce a certificate issued by a competent authority as per the Government of India Guidelines(wherever applicable).
12. Only persons with **benchmark disabilities** would be eligible for reservation under PwBD category. "**Benchmark disability**" means a person with not less than 40% of a specified disability where specified disability has not been defined in measurable terms and includes the persons with disability, where disability has been defined in a measurable term, as certified by the certifying authority. A person who wants to avail the benefit of reservation will have to submit latest Disability Certificate, on prescribed format, issued by Medical Authority or any other notified Competent Authority (Certifying Authority). **The certificate should be dated on or before last date of registration of application. In absence of valid certificate, the candidature will be liable for cancellation / rejection and no communication in this regard will be entertained by the Bank.** Horizontal reservation has been provided to Persons with Benchmark Disabilities as per section 34 of "The Rights of Persons with Disabilities Act (RPWD), 2016". Suitable categories of disabilities and Functional requirements for the post(s) will be in reference to the Gazette of India, Notification No. 38-16/2020-DD-III dated 4th January 2021, Ministry of Social Justice and Empowerment [Department of Empowerment of Persons with Disabilities (Divyangjan)].

(B) Details of Educational Qualification/ Certification/ Work Experience/ Specific Skills Required:

Post No / Post Name	1 – Deputy Manager- IT Security Expert
BASIC QUALIFICATION **(AS ON 31.01.2026)**	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER CERTIFICATIONS **(AS ON 31.01.2026)**	**Preferred Certifications:** (Valid as on 31.01.2026) OSCP, CEH, CHFI, GIFR, GIACC, GFSU.
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.01.2026)**	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** Experience in Cyber Defence operations (Threat Intel), Incident Response, Malware Analysis, Forensics, Threat Hunting **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of job, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of job and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Expertise in incident response, malware analysis, digital forensics, and cyber threat hunting. • Understanding of cloud, OT/ICS, and IoT security, red teaming, IR, Ethical hacking. • Strong technology leadership, people management, and stakeholder engagement skills. • Ability to handle high-pressure cyber crisis situations. • Excellent written and verbal communication, including ability to brief senior executives and policymakers.

Post No / Post Name	2 – Deputy Manager -Emerging Technology
BASIC QUALIFICATION **(AS ON 31.01.2026)**	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER CERTIFICATIONS **(AS ON 31.01.2026)**	**Preferred Certifications:** (Valid as on 31.01.2026) • Equivalent certifications in Innovation, Product Development, Web development etc in cyber security. • Java developer, mobile developer, Python developer, Web developer.
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.01.2026)**	**Mandatory:** Minimum Experience: 4 years of post-qualification experience in the Cybersecurity/Technology Innovation domain. **Preferred:** Hands-on work experience Preferably in cyber innovation labs. Product evaluation, prototyping, or applied cybersecurity solutioning is preferred.

	Exposure to handling R&D or applied Technology problem statements and experience in innovation environment is an added advantage. Cyber research, threat intelligence research etc. Understanding of cyber security principles, threat landscapes, and information security technologies. **<u>Training & Teaching experience will not be counted for eligibility</u>.** **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Ability to think creatively and develop original, effective solutions for complex security challenges. • Strong ability to analyze security incidents and assess the efficacy of new technologies and strategies. • A continuous learning mindset to stay abreast of cutting-edge technologies and evolving threats. • Strong understanding of emerging technologies: Artificial Intelligence (AI/ML), Blockchain, Quantum Computing, Cloud Security. • Proficiency in cyber threat modelling, simulation, and scenario-based evaluation. • Capability in prototyping, product validation, and applied research. • Ability to work with startups, academic institutions, and fintech innovators to co-develop solutions. • Excellent analytical, technical writing, and presentation skills. • Ability to translate innovation into deployable solutions aligned with the Bank's cybersecurity posture. • Exposure to banking, financial institutions (FIs), or PSU-led cybersecurity innovation projects. • Collaboration with academia, start-ups, and incubators in emerging technology/cybersecurity innovation. • Ability to contribute to national/international research initiatives or patents in technology/cybersecurity. • Ability to conduct deep-dive research on emerging cyber threats, tools, and trends • Experience with open-source intelligence (OSINT) tools and techniques • Data collection, synthesis, and interpretation from technical and non-technical sources. • Understanding of cybersecurity principles, technologies, and best practices, including network security, cloud security, endpoint security, and incident response. • Find security flaws in systems, applications, and networks before they can be exploited by malicious actors. • Create proof-of-concept exploits to demonstrate the real-world impact of vulnerabilities, helping to justify the need for security solutions • Ability to conduct research, analyse data, and identify innovative solutions or ideas to address complex cybersecurity challenges. • Ability to effectively communicate complex technical information to both technical and non-technical audiences. • Ability to identify and solve complex cybersecurity problems. • Driven by a deep curiosity to understand how systems work and have the persistence to investigate complex problems.

Post No / Post Name	**3 – Deputy Manager -Cyber Security Analyst**
BASIC QUALIFICATION **(AS ON 31.01.2026)**	**<u>Mandatory:</u>** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **<u>Preferred:</u>** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER CERTIFICATIONS **(AS ON 31.01.2026)**	**<u>Preferred Certifications:</u>** (Valid as on 31.01.2026) OSCP, OSCE, CRTE, CRTP, CEH, CISSP, OSEP, CCSP, SANS.
WORK EXPERIENCE **(POST-BASIC QUALIFICATION)** **(AS ON 31.01.2026)**	**<u>Mandatory:</u>** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain.

	Preferred: Experience in offensive security, focusing on Ethical Hacking red teaming and penetration testing. **Training & Teaching experience will not be counted for eligibility.** **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Understanding of IT Security technology & processes particularly related to Web/Mobile Applications and Network Security. • Understanding of OWASP Web and Mobile Top 10 Application Security Vulnerabilities, Threat modelling, Red Teaming & Secure code review. • Ability to perform security assessment of Web and Mobile (Android and iOS) applications to identify OWASP Top 10 related vulnerabilities. • Knowledge of tools like Kali Linux, Burp suite, Nmap, Qualys/Nessus, Metasploit, HCL AppScan, Tenable SC, NMAP, etc. • Basic Knowledge of at least one programming knowledge such as C, C++, Python, Java, ASP.NET will be preferred. • Hands-on security testing of mobile applications (Static/ Dynamic/Memory Analysis) and experience on Dynamic instrumentation tools like Frida/Objection, Magisk etc. Knowledge on Android Development tools. • Proficiency in languages such as Python, Bash/Shell, C/C++, Java, and JavaScript, Burp Suit, Kali-Linux is crucial for scripting, automation, exploit development, and understanding system vulnerabilities. • Expertise in various penetration testing & red Team Testing methodologies (MITRE, OWASP Testing Guide, NIST SP 800-115, etc.), tools (Nmap, Metasploit, Burp Suite, Wireshark, John the Ripper, etc.), and techniques (reconnaissance, scanning, exploitation, post-exploitation, privilege escalation) • Knowledge of wireless protocols (Wi-Fi), security standards (WPA2, WPA3), and hacking methods (packet sniffing, encryption cracking). • Ability to analyse complex situations, identify challenges, and devise effective and innovative solutions through critical and lateral thinking, coupled with a knack for identifying potential security risks.

Post No / Post Name	**4 – Deputy Manager -Incident Management & Forensics**
BASIC QUALIFICATION (AS ON 31.01.2026)	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER QUALIFICATION (AS ON 31.01.2026)	**Preferred Certifications:** (Valid as on 31.01.2026) CHFI, Encase Certified Examiner (EnCE), Access Data Certified Examiner (ACE), GIAC Certified Incident Handler (GCIH). Certified Information Systems Security Professional (CISSP), GIAC Certified Forensic Analyst (GCFA). CEH, OSCP, OCEP.
WORK EXPERIENCE (POST-BASIC QUALIFICATION) (AS ON 31.01.2026)	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** Experience in Incident Response, forensic and malware Analysis. With hands-on experience in malware analysis, digital forensics, mobile forensics, Network forensics, Database forensics, Email forensics, cloud forensics. experience in cybersecurity, with a strong focus on incident response and security operations.

	Experience with various security incidents, such as malware, ransomware, phishing, DDoS attacks, and data breaches. **<u>Training & Teaching experience will not be counted for eligibility</u>**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	**Core Forensic Skills** • **Digital Forensics:** Expertise in acquiring, preserving, analysing, and reporting digital evidence from devices, servers, and networks. • Detection & Investigation: In-depth knowledge of detecting, investigating, and documenting fraud schemes such as money laundering, insider trading, and cyber frauds. • Incident Response: Ability to Execute and investigate data breaches, cyber incidents, and security threats efficiently. **Technical Skills** • **Forensic Tools Expertise:** EnCase, FTK, Magnet Axiom, X-Ways, Autopsy, Wireshark, Cellebrite, Oxygen Forensics (for mobile forensics) etc. • Forensic Imaging Tools: Tableau TX1/TDU/write blockers, Logicude Image etc. • SIEM & Threat Intelligence Tools: Splunk, IBM QRadar, ArcSight • Data Analysis & Scripting: SQL for data extraction from core banking systems • Python, PowerShell for scripting and automation • Malware Analysis & Reverse Engineering (preferred for cyber forensics roles) **BFSI, Regulatory & Legal Domain Knowledge** • Understanding of Financial Products & Systems • RBI Guidelines on Cybersecurity & Forensics • SEBI and IRDAI regulations • Chain of Custody: Ability to maintain legally admissible evidence trails • Report Writing: Skill in preparing detailed forensic reports and executive summaries. • Excellent communication and presentation skills. Ability to effectively communicate technical information to both technical and non-technical audiences. • Knowledge of network protocols and operating systems. • Hands-on experience in malware analysis, digital forensics, mobile forensics, Network forensics, Database forensics, Email forensics, cloud forensics. • Execute and coordinate the full lifecycle of cybersecurity incidents – identification, containment, eradication, recovery, and post-incident analysis. • Act as the primary responder for high-severity security incidents including malware outbreaks, DDoS, ransomware, phishing, data breaches, and insider threats. • Monitor and analyse logs and alerts from SIEM tools (e.g., Splunk, QRadar, ArcSight) to detect anomalies and potential threats across endpoints, networks, and applications. • Develop and maintain incident playbooks, escalation protocols, and response workflows in line with RBI cybersecurity directives. • Perform forensic analysis on compromised systems to determine the root cause, impact, and indicators of compromise (IOCs). • Collaborate with SOC analysts, threat intelligence teams, IT, legal, and external vendors during incident handling. • Prepare detailed incident reports and dashboards for senior management and regulators (e.g., RBI, SEBI). • Conduct post-incident reviews (PIRs) and contribute to improving the security posture through lessons learned and preventive controls. • Support compliance initiatives by aligning incident response processes with ISO 27001, RBI cybersecurity framework, NIST, and CERT-In advisories. • knowledge of incident response methodologies, frameworks, and best practices (e.g., NIST, ISO 27001, MITRE ATT&CK). • Proficiency with incident response tools and technologies, including SIEM, EDR, forensics tools, and security orchestration and automation (SOAR) platforms. • Solid understanding of networking, operating systems (Windows, Linux), cloud platforms (e.g., AWS, Azure, GCP), and security vulnerabilities.

	• Experience with scripting or programming languages (e.g., Python, PowerShell) for automation and analysis is a plus. • Excellent written and verbal communication skills, including the ability to communicate technical information effectively to both technical and non-technical stakeholders, including senior leadership. • Exceptional analytical, problem-solving, and decision-making abilities, with the capacity to think critically and strategically under pressure. • Ability to prioritize and manage multiple incidents concurrently, demonstrating strong organizational and time management skills.

Post No / Post Name	**5 – Deputy Manager -Test Engineers**
BASIC QUALIFICATION (AS ON 31.01.2026)	**Mandatory:** B.Tech/ B.E. in Computer Science/ Computer Science & Engineering/ Software Engineering/ Information Technology/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines **with minimum 50% score**. or MCA or M. Tech/ M. Sc in Computer Science/ Computer Science & Engineering/ Information Technology/ Software Engineering/ Electronics/ Electronics & Communications Engineering or Equivalent Degree in above specified disciplines. (From a University/ Institution/ Board recognized by Govt. Of India/ approved by Govt. Regulatory Bodies). **Preferred:** **An advanced degree in Cybersecurity or Information Technology, would be preferred.**
OTHER QUALIFICATION (AS ON 31.01.2026)	**Preferred Certifications:** (Valid as on 31.01.2026) ISTQB, STQC STANDARD MAPPING, CTFL, CSTE, CAST, CISSP, CISM, Technology Hardware related certifications are preferred.
WORK EXPERIENCE (POST-BASIC QUALIFICATION) (AS ON 31.01.2026)	**Mandatory:** Minimum Experience: 4 years post-qualification experience in the Cyber Security / Information Technology Domain. **Preferred:** Experience testing hardware / software and finding bugs. Must have experience in designing and executing test plans and procedures. This includes creating automated tests using scripting languages like Python. Needs strong debugging and troubleshooting skills to perform root-cause analysis of hardware/ software issues. Analysis of technology products and services. Experience as an analyst in a finance, business, or operational/technology setting. **Training & Teaching experience will not be counted for eligibility**. **Note:** Candidates are required to produce up-to-date and full Experience Certificate, unambiguously indicating: (i) Nature of duties, (ii) Dates and duration of experience, (iii) Level / position, (iv) Responsibilities etc. issued by the employer(s). However, if the candidate is unable to submit an Experience Certificate on the lines indicated above, any document unambiguously indicating the experience, nature of duties and the period claimed may be submitted and it would be considered on merit at the discretion of the Bank and the decision of the Bank shall be final.
SPECIFIC SKILLS	• Strong understanding of hardware design principles, computer architecture, and electrical/electronic systems. • Experience with hardware testing methodologies, test equipment, and test automation tools. • Excellent analytical and problem-solving skills to diagnose and troubleshoot hardware faults. • Strong communication and documentation skills for creating clear and concise test plans and reports. • The ability to work in a fast-paced, dynamic environment and adapt to changing project requirements. • Strong understanding of computer hardware, hardware testing, and analysis, along with strong problem-solving, critical-thinking, and communication abilities to evaluate hardware, design systems, manage upgrades, and assist users. • **Programming and Scripting:** Knowledge of languages like Java or Python helps testers understand the software's architecture and automate tests. • **Operating Systems:** Familiarity with various OS platforms like Windows, macOS, Linux, iOS, and Android ensure compatibility testing. • **Test Automation Tools:** Proficiency with tools for test case management, defect tracking, and automation is essential for efficiency.

	• **Analytical & Critical Thinking:** The ability to meticulously assess software, break down complex problems, and identify root causes of defects. • **Communication:** Strong verbal and written skills are needed to communicate findings, document issues clearly, and collaborate effectively with development teams. • **Problem-Solving:** Testers must be able to systematically find solutions to issues encountered during the testing process. • **Attention to Detail:** A keen eye for detail is crucial for accurately identifying and documenting all defects and their nuances. • **Adaptability and Flexibility:** The software landscape is constantly changing, requiring testers to be adaptable and willing to learn new technologies and methodologies. • **User-Centric Mindset:** A focus on meeting user needs ensures the final software product is high-quality and user-friendly. • Strong analytical and problem-solving skills with a high degree of accuracy and attention to detail. • Adept at interpreting complex data, identifying trends, and proposing effective solutions. • Expertise in Microsoft Excel for data modelling, analysis, and reporting. • Proficiency with business intelligence (BI) and data visualization tools (e.g., Power BI, Tableau). • Excellent written and verbal communication skills. • Strong stakeholder management skills with the ability to influence and collaborate effectively across different teams and levels. • Builds and maintains strong, collaborative relationships with internal and external partners. • Understands business needs and strategic objectives to clarify the purpose of benchmarking efforts.

IMPORTANT POINTS:

1 The educational qualification prescribed for the post is minimum. Candidate must possess the Post Basic qualification and relevant full-time experience as on specified dates.

2 **The relevant experience certificate from the employer must contain specifically that the candidate had experience in that related field as required.**

3 In cases the certificate of degree/diploma does not specify the field of specialization, the candidate will have to produce a certificate from the concerned university/college specifically mentioning the specialization.

C. DETAILS OF BRIEF JOB PROFILE, ROLE & RESPONSIBILITIES, FUNCTIONS & ACTIVITIES:

Sl	POST	Detail description of Job Profile, Role, Responsibilities, and Functions.
1.	**Deputy Manager-** **IT Security Expert**	**Job Profile:** The IT Security Experts will operate as Cyber Defense Specialists and will execute the operations of the Cyber Defense Centre within the Cyber Security Centre of Excellence. The role involves building, managing, and operating advanced cyber defense capabilities covering Threat Intelligence, Incident Response, and Cyber Resilience functions. He/She will be responsible for monitoring, detecting, analyzing, and responding to cyber threats while ensuring compliance with regulatory and organizational requirements. **KRAs:** **On Ground Execution:** • Work with team of Cyber analysts, threat hunters, incident responders, and security engineers. • Drive collaboration with government agencies, regulators, industry partners, and academia. **Operational Management** • Ensure timely detection, triage, and response to security incidents. • Develop and implement playbooks for Incident Response and Cyber Crisis Management. • Manage Threat Intelligence lifecycle: collection, analysis, dissemination, and actioning. • Oversee vulnerability management and proactive threat hunting initiatives. • Maintain cyber resilience by conducting red team/blue team exercises, simulations, and drills. **Governance & Compliance** • Ensure alignment to national and international cybersecurity standards (ISO 27001, NIST, CERT-In guidelines, RBI/SEBI/MeitY advisories). • Prepare periodic risk, threat, and incident reports for leadership and regulatory bodies. • Support audits, compliance assessments, and cybersecurity maturity evaluations. **Capacity Building & Innovation** • Contribute to the CoE's knowledge repository through research, frameworks, and best practices. • Mentor and upskill team members on emerging cyber defense technologies (AI/ML in security, SOAR, SIEM, XDR, Cloud Security). • Foster innovation by engaging with startups, academia, and global cyber defense forums.

2.	Deputy Manager – Emerging Technology	**Job Profile:** It identifies, develops, and implements new strategies, technologies, and methodologies to enhance an organization's security posture against evolving cyber threats. They are responsible for leading cybersecurity initiatives, assessing new solutions, and ensuring that an organization remains resilient and secure in a dynamic threat landscape, requiring technical expertise and an innovative mindset to create novel approaches to threat management. It will play a key role in bridging business needs with technology or cyber solutions. The analyst works closely with business units, developers and project teams to ensure that technology / cyber initiatives align with organizational goals. Drive Cybersecurity innovation and applied research in the cybersecurity domain. Conduct evaluation of emerging security technologies and assess applicability in the banking environment. Build proof-of-concepts (PoCs) and pilot projects for advanced cybersecurity solutions. Engage with start-ups, incubators, and research institutions to scout, validate, and adapt innovative solutions. Assist in designing in-house tools, frameworks, and methodologies for cybersecurity innovation. Is responsible for collecting, analysing and interpreting data to help organizations make informed decisions. The role requires strong analytical and communications skills, attention to detail, and the ability to transform complex data into actionable insights. This role involves carrying out research initiatives, driving innovation in cybersecurity, and ensuring the organization's cyber defenses are robust and effective. **KRAs:** **Technology Analysis & Evolution:** • Evaluate new and existing technologies to determine suitability and potential impact on the business requirements. • Stay ahead of the curve by anticipating new cyber threats and vulnerabilities in the digital landscape. • Conduct feasibility studies and cost benefit analysis for technology /Cyber solutions. • Research, design, and implement innovative technical solutions and frameworks to strengthen cybersecurity defense. • Spearhead projects that introduce cutting-edge technologies and processes to protect networks, systems, and data. **Business and systems analysis:** • Collaborate with business stakeholders to gather and analyse technical and business requirements. • Translate business needs into functional and technical specifications. • Support business process reengineering and digital transformation initiatives. **Solution Design & implementation Support:** • Design system architectures, data flows and integration points. • Work with software developers, IT-Engineers and vendors during implementations. • Ensure solutions meet business, technical and compliance requirements. **Technical Documentations & Reporting:** • Prepare system and process documentations user guides and technical manuals. • Provide technical reports and dashboards to management stakeholders. • Present findings, technology options and recommendations in a clear business friendly manner. • Engage with internal and external stakeholders, including research institutions and industry partners, to foster a collaborative ecosystem for cybersecurity innovation. **Planning:** Developing and implementing the center's strategic vision and roadmap for cybersecurity research and development. **Research and Innovation:** Overseeing research projects focused on identifying and mitigating emerging cyber threats, developing new security technologies, and enhancing existing security protocols. **Collaboration and Partnerships:** Working with internal teams, external research institutions, and industry partners to advance cybersecurity knowledge and capabilities. **Knowledge Sharing:** Disseminating research findings and best practices throughout the organization and potentially to the broader cybersecurity community. **Staying Ahead of Threats:** Keeping abreast of the latest cybersecurity trends, threats, and technologies to ensure the organization remains protected.

		Cybersecurity Research & Intelligence: Conduct ongoing research on emerging cybersecurity threats, vulnerabilities, tools, technologies, and best practices. Monitor cybersecurity developments across academic, government, and industry sources. Compile research findings into actionable insights for internal stakeholders. Provide research-based insights to support strategic planning, capability development, and investment decisions for cybersecurity initiatives.
3.	Deputy Manager – Cyber Security Analyst	**<u>Job Profile:</u>** The Ethical Hacking & Red Team Analyst, embedded within the Cybersecurity Centre of Excellence, will be responsible for proactively identifying, exploiting, and providing actionable intelligence on security vulnerabilities across the organization's infrastructure, applications, mobile apps and processes. This role will simulate real-world attacks, conduct advanced penetration testing, and contribute to enhancing the organization's overall security posture. The specialist will play a key role in developing and refining the CoE's red teaming methodologies and capabilities, fostering a culture of security awareness and resilience. **<u>KRAs:</u>** **Red Teaming & Adversary Simulation:** Planning and executing red team engagements to test security controls against realistic attack scenarios, utilizing custom exploits and techniques that mimic advanced threat actors by leveraging red teaming testing techniques MITRE ATT&CK frameworks. **Penetration Testing:** Performing in-depth penetration tests & exploitation of networks, applications, mobile app, and systems using automated and manual methods to identify complex vulnerabilities. **Vulnerability Research & Exploit Development:** Staying updated on threats and developing custom exploits to test vulnerabilities & identify zero-day vulnerabilities. **Secure Code Review:** Reviewing code for vulnerabilities from an attacker's perspective. **Bug Bounty:** To find and report security vulnerabilities in their software or systems, helping them identify and fix flaws before malicious actors can exploit them. **Vulnerability Management:** Validating and verifying the effectiveness of vulnerability remediation. **Collaboration & Communication:** Working with other teams to improve security and clearly documenting and presenting findings. **Security Tooling & Automation:** Evaluating and automating offensive security tools and processes. **Continuous Learning & Research:** Staying informed on security trends and participating in cybersecurity communities.
4.	Deputy Manager – Incident Management & Forensics	**<u>Job Profile:</u>** This is critical role, responsible for overseeing the entire incident response lifecycle, ensuring rapid detection, containment, eradication, ransomware, and recovery from cyberattacks and security breaches across the organization. You will lead, mentor, and empower a team of dedicated IR specialists, define and refine incident response processes, framework, SOPs and playbooks, and foster a culture of preparedness, continuous improvement, and collaborative defense against evolving cyber threats. In a Center of Excellence (COE) he will be responsible for investigating security incidents, analyzing malware, and developing strategies to improve the organization's security posture. This role requires strong technical expertise in malware analysis and digital forensics.

KRAs:

- Execute end-to-end forensic investigations involving cyber incidents, fraud, data leakage, and policy violations within the organization.
- Perform digital evidence acquisition, preservation, and analysis across various systems, including endpoint devices, servers, cloud platforms, and mobile devices.
- Investigate financial frauds, insider threats, and anomalies in payment systems using core banking and transaction data.
- Prepare detailed forensic reports, timelines, and exhibits for internal reviews, legal proceedings, and regulatory bodies (e.g., RBI, SEBI).
- Collaborate with internal teams (Legal, Compliance, Risk, and IT Security) to support investigations and ensure regulatory compliance.
- Provide expert support in responding to cybersecurity incidents including root cause analysis and recommendations for corrective actions.
- Ensure all forensic investigations are conducted in accordance with Indian cyber laws and evidence handling best practices.
- Maintain forensic toolsets and keep up-to-date with emerging threats, techniques, and regulatory guidelines.
- Execute digital forensics and cyber investigations, which involves overseeing various incidents, directing forensic processes and evidence handling, coordinating with legal and law enforcement, and leading investigations into advanced threats.
- Malware analysis and threat intelligence, encompassing supervising analysis and reverse engineering, collaborating with threat intelligence teams, and refining incident response protocols.
- Focused on managing and mentoring forensic analysts, providing technical guidance, and conducting performance reviews.
- Incident response and security posture enhancement, acting as an escalation point, overseeing analysis updates, supporting readiness initiatives, coordinating with vendors, and representing the function in various engagements.
- Documentation and reporting, ensuring detailed reports and maintaining records for legal and audit purposes.
- Perform end to end digital forensics across endpoints, servers, mobile devices and cloud platforms.
- Conduct forensic imaging, log analysis and artifact extraction to support investigations.
- Provide forensics reports for internal stakeholders, legal and regulatory bodies.
- Analyse and reverse engineer malicious code, scripts and exploits.
- Use sandboxing, static/dynamic analysis and debugging tools to understand the behaviour of malware.
- Provide forensics and malware analysis expertise during incident response engagements.
- Contribute to threat intelligence feeds by sharing malware insights.
- Participate in table- top exercise and threat simulations.

Incident Response & management:

- Execute and manage the incident response team, overseeing all phases of the incident response lifecycle, including detection, analysis, containment, eradication, recovery, and post-incident activities.
- Coordinate incident response efforts across cross-functional teams, including IT operations, security operations, legal, and communications, to ensure a unified and effective response during critical incidents.
- Serve as the primary point of contact and escalation for high-priority incidents, providing guidance and decisive leadership to the incident response team and stakeholders.

Strategy, process & playbook development:

- Develop, implement, and continuously refine the organization's incident response strategy, processes, procedures, and playbooks, ensuring alignment with industry best practices (e.g., NIST, ISO 27001) and regulatory requirements.
- Drive the development and maintenance of comprehensive incident response plans, procedures, and runbooks tailored to different types of security incidents and organizational assets.

		• Implement and leverage incident management platforms and tools (e.g., SIEM, EDR, SOAR) to streamline incident detection, analysis, and response workflows. **Investigation & forensics:** • Oversee in-depth investigations and forensic analysis to determine the root cause, scope, and impact of security incidents. Ensure proper collection, preservation, and analysis of digital evidence, adhering to legal and forensic standards. • Collaborate with legal counsel and law enforcement agencies when necessary, ensuring compliance with legal requirements and reporting obligations. **Team development & mentorship:** • Work with team of incident response specialists, fostering a high-performing, collaborative, and learning-focused environment. • Develop and deliver training programs, workshops, and tabletop exercises to enhance the skills, knowledge, and preparedness of the incident response team. • Conduct performance reviews, provide constructive feedback, and support the professional growth and career development of team members Continuous. **improvement & reporting:** • Post-incident review (PIR) and "lessons learned" sessions to identify areas for improvement in incident response processes, technologies, and team capabilities. • Develop and present incident reports and briefings to senior management and stakeholders, highlighting incident trends, risks, and recommendations for remediation and prevention.
5.	Deputy Manager – Test Engineers	**Job Profile:** This role analyzes data to identify internal and external operational and performance gaps, fosters continuous improvement, and provides actionable insights for strategic decisions, often requiring strong analytical, communication, and project management skills to collaborate with stakeholders and drive improvements in efficiency and performance against industry best practices. This role is responsible for evaluating, testing, and validating hardware components and systems to ensure they meet performance, reliability, and quality standards before product release. This role combines technical expertise with strong analytical and problem-solving skills to identify and troubleshoot issues throughout the product lifecycle. This role involves analysing requirements, designing test plans and cases, setting up test environments, executing various types of tests (functional, performance, security), logging defects, and communicating results to stakeholders to ensure software quality and reliability. Key responsibilities include collaborating with developers, validating functionality across platforms, identifying usability issues, and participating in design reviews to provide input for improving the product. **KRAs:** • Arrange project requirements in programming sequence by analysing requirements, preparing a work flow chart and diagram using knowledge of computer capabilities, subject matter, programming language, and logic. • Maintain, manage and modify all software systems, tools, and applications. • Develop and analyze functional specifications. • Be the interface between end-users and software consultants. • Resolve complex issues relating to business requirements and objectives. • Coordinate and support software professionals in installing and analyzing applications and tools. • Develop, analyze and implement testing procedures, programming, and documentation. • Train and develop other software analysts. • Analyze, design, and develop modifications and changes to existing systems to enhance performance. • Software benchmarking: measure a software's performance, such as its speed, stability, and resource usage, against established standards or competitors to identify areas for improvement. It involves establishing quantifiable metrics and test environments to compare a software application's performance against defined goals or industry averages, ultimately guiding optimization and ensuring it meets desired quality standards before release. **Benchmarking:** • Evaluating individual hardware components and modules, such as CPUs, GPUs, memory, and storage devices. • This type of testing measures raw power and efficiency, giving insight into how well each component performs under various conditions.

		Hardware Evolution & Installation: • Assess organizational needs to recommend hardware upgrades or new acquisitions. • Install and configure hardware compliance with company standards and compatibility with existing systems. • Ensure hardware compliance with company standards and compatibility with existing systems. **Test Planning & Design:** • Create comprehensive test plans, test cases, and test strategies based on hardware design specifications and customer requirements. • One of the most common and convenient ways to test and evaluate hardware performance is to use benchmarking tools. • Benchmarking tools are software applications that run standardized tests on your hardware and generate scores and metrics that reflect its capabilities. **Benchmarking & Performance Analysis:** • Identify relevant internal metrics and external benchmarks for performance comparison. • Conduct comparative analyses against industry peers, competitors, or global standards. • Evaluate performance gaps and recommend improvement opportunities. **Continuous Improvement:** Drive initiatives to improve performance and optimize results by implementing solutions based on data insights. **Stakeholder Collaboration:** Work closely with cross-functional teams (e.g., Marketing, Sales, Operations, Finance) to gather data, share insights, and align on improvement strategies. **Strategic Insights:** Provide actionable recommendations to management to inform strategic planning, growth initiatives, and operational efficiency. **Process Optimization:** Support the development and implementation of frameworks for measuring performance against set goals and user needs **Data Management and Quality:** • Ensure the availability and quality of data used for benchmarking, working with data teams to resolve inconsistencies. • Perform quality assurance on data and reports to ensure accuracy and integrity. • Document benchmarking processes, methodologies, and identified issues. **Process Improvement and Strategy:** • Leverage benchmarking insights to recommend strategic initiatives for process optimization and improved operational efficiency. • Support the CoE in developing and refining the overall benchmarking strategy and methodology. • Facilitate workshops and meetings to discuss benchmarking results and drive action plans. **Reporting & Insights Generation:** • Develop dashboards, reports, and presentations to communicate findings and KPIs. • Translate complex data into clear insights and narratives for stakeholders and leadership. • Track trends and identify areas of competitive advantage or risk.

Remarks: Actual KRAs shall be assigned on joining. Roles / Responsibilities / Job Profile mentioned above are illustrative. Roles / Responsibilities / Activities / Key Interactions/ Jobs in addition to the above mentioned may be assigned by the Bank from time to time depending upon the requirement.

The candidates selected on Regular posts will be governed by the Service Rules applicable to the employees of the SBI.

(D) REMUNERATION /SUGGESTED PLACE OF POSTING:

Sl. No.	Name of Post	Grade	Scale of Pay	Place of Posting
1.	Deputy Manager- IT Security Expert	MMGS-II	**Basic: 64820-2340/1-67160-2680/10-93960** (The official will be eligible for DA, HRA, CCA, PF, Contributory Pension Fund i.e., NPS, LFC, Medical Facility, leave etc. as per rules in force from time to time and Salary and perks as per Bank's salary structure)	Mumbai or anywhere in India, in case of any administrative requirement.
2.	Deputy Manager -Emerging Technology			
3.	Deputy Manager -Cyber Security Analyst			
4.	Deputy Manager -Incident Management & Forensics			
5.	Deputy Manager -Test Engineers			

E. <u>SELECTION PROCESS</u>: The selection will be on the basis of **Shortlisting and Interview.**

- **Shortlisting**: **Mere fulfilling the minimum qualification and experience will not vest any right to candidate for being called for interview.** The shortlisting committee constituted by the Bank will decide the shortlisting parameters and thereafter, adequate number of candidates, as decided by the Bank, will be shortlisted for interview. The decision of the Bank to call the candidates for the interview shall be final. No correspondence will be entertained in this regard.
- **Interview:** Interview will carry 100 marks. The qualifying marks in interview will be decided by the Bank. No correspondence will be entertained in this regard.
- **Merit List:** Merit list for selection will be prepared in descending order based on scores obtained in interview only. In case more than one candidate score the cut-off marks (common marks at cut-off point), such candidates will be ranked according to their age in descending order, in the merit list.

F. <u>CALL LETTER FOR INTERVIEW:</u> Intimation/call letter for interview will be uploaded on bank's website or sent by email, as decided by the Bank. **NO HARD COPY WILL BE SENT.**

G. HOW TO APPLY: Candidates should have **valid Email ID** which should be kept active till the declaration of result. It will help him/her in getting call letter/ **i**nterview advice etc. by email.

GUIDELINES FOR FILLING ONLINE APPLICATION	GUIDELINES FOR PAYMENT OF FEES
i. Candidates will be required to register themselves online through the link available on SBI website **https://sbi.bank.in/web/careers/current-openings** and pay the application fee using Internet Banking/ Debit Card/ Credit Card/ UPI etc. ii. Candidates should first scan their latest photograph and signature. Online application will not be registered unless candidate uploads his/ her photo and signature as specified on the online registration page (under 'How to Upload Document"). iii. Candidates should fill the application carefully. Once application is filled-in completely, candidate should submit the same. In the event of candidate not being able to fill the application in one go, he can save the information already entered. When the information/ application is saved, a provisional registration number and password is generated by the system and displayed on the screen. **Candidate should note down the registration number and password.** They can re-open the saved application using registration number and password and edit the particulars, if needed. This facility of editing the saved information will be available for three times only. Once the application is filled completely, candidate should submit the same and proceed for online payment of fee. iv. **After registering online, the candidates are advised to take a printout of the system generated online application form.** v. Candidates seeking Age relaxation are required to submit copies of necessary certificates at the time of document verification. No change in category of any candidate is permitted after registration of online application.	i. Application fees and Intimation Charges (Non-refundable) is ₹ 750/- (₹Seven Hundred Fifty only) for General/EWS/OBC candidates and no fees/intimation charges for SC/ ST /PwBD candidates. ii. After ensuring correctness of the particulars in the application form, candidates are required to pay the fees through payment gateway integrated with the application. No change/ edit in the application will be allowed thereafter. iii. Fee payment will have to be made online through payment gateway available thereat. The payment can be made by using Debit Card/ Credit Card/ Internet Banking/ UPI etc. by providing information as asked on the screen. Transaction charges for online payment, if any, will be borne by the candidates. iv. On successful completion of the transaction, e-receipt and application form, bearing the date of submission by the candidate, will be generated which should be printed and retained by the candidate. v. If the online payment of fee is not successfully completed in first instance, please make fresh attempts to make online payment. vi. A provision is there to reprint the e-Receipt and Application form containing fee details, at later stage. vii. **Application Fee once paid will NOT be refunded on any account NOR can it be adjusted for any other examination or selection in future.**

H. HOW TO UPLOAD DOCUMENTS:

a. Details of Document to be uploaded:	d. Document file type/ size:
i. Recent Photograph ii. Signature iii. Biodata (Format Attached) (PDF) iv. Resume (PDF) v. ID Proof (PDF) vi. Proof of Date of Birth (PDF) vii. Educational Certificates: Relevant Mark-Sheets/ Degree Certificate (PDF) viii. Experience certificates (PDF) ix. Caste Certificate / EWS Certificate (if applicable) (PDF) x. PwBD Certificate (if applicable) (PDF) xi. Preferred qualification / Certification (if any) (PDF) xii. Form-16/Offer Letter/Latest Salary slip from current employer (PDF)	i. All Documents must be in PDF (except Photograph & Signature) ii. Page size of the document to be A4 iii. Size of the file should not be exceeding 500 kb. iv. In case of Document being scanned, please ensure it is saved as PDF and size not more than 500 kb as PDF. If the size of the file is more than 500 kb, then adjust the setting of the scanner such as the DPI resolution, no. of colors etc., during the process of scanning. Please ensure that Documents uploaded are clear and readable.

b. Photograph file type/ size:

i. Photograph must be a recent passport style colour picture.
ii. Size of file should be between 20 kb - 50 kb and Dimensions 200 x 230 pixels (preferred)
iii. Make sure that the picture is in colour, taken against a light-coloured, preferably white, background.
iv. Look straight at the camera with a relaxed face
v. If the picture is taken on a sunny day, have the sun behind you, or place yourself in the shade, so that you are not squinting and there are no harsh shadows
vi. If you have to use flash, ensure there's no "red-eye"
vii. If you wear glasses make sure that there are no reflections, and your eyes can be clearly seen.
viii. Caps, hats and dark glasses are not acceptable. Religious headwear is allowed but it must not cover your face.
ix. Ensure that the size of the scanned image is not more than 50kb. If the size of the file is more than 50 kb, then adjust the settings of the scanner such as the DPI resolution, no. of colour etc., during the process of scanning.

c. Signature file type/ size:

i. The applicant has to sign on white paper with Black Ink pen.
ii. The signature must be signed only by the applicant and not by any other person.
iii. The signature will be used to put on the Call Letter and wherever necessary.
iv. Size of file should be between 10 kb - 20 kb and Dimensions 140 x 60 pixels (preferred).
v. Ensure that the size of the scanned image is not more than 20 kb.
vi. **Signature in CAPITAL LETTERS shall NOT be accepted**.

e. Guidelines for scanning of photograph/ signature/ documents:

i. Set the scanner resolution to a minimum of 200 dpi (dots per inch)
ii. Set Color to True Color
iii. Crop the image in the scanner to the edge of the photograph/ signature, then use the upload editor to crop the image to the final size (as specified above).
iv. The photo/ signature file should be JPG or JPEG format (i.e. file name should appear as: image01.jpg or image01.jpeg).
v. Image dimensions can be checked by listing the folder/ files or moving the mouse over the file image icon.
vi. Candidates using MS Windows/ MSOffice can easily obtain photo and signature in .jpeg format not exceeding 50 kb & 20 kb respectively by using MS Paint or MSOffice Picture Manager. Scanned photograph and signature in any format can be saved in .jpg format by using 'Save As' option in the File menu. The file size can be reduced below 50 kb (photograph) & 20 kb (signature) by using crop and then resize option (Please see point (i) & (ii) above for the pixel size) in the 'Image' menu. Similar options are available in another photo editor also.
vii. While filling in the Online Application Form the candidate will be provided with a link to upload his/her photograph and signature.

f. Procedure for Uploading Document:

i. There will be separate links for uploading each document.
ii. Click on the respective link "Upload"
iii. Browse & select the location where the JPG or JEPG, PDF etc. file has been saved.
iv. Select the file by clicking on it and click the 'Upload' button.
v. Click Preview to confirm the document is uploaded and accessible properly before submitting the application. If the file size and format are not as prescribed, an error message will be displayed
vi. Once uploaded/ submitted, the Documents uploaded cannot be edited/ changed.
vii. **After uploading the photograph/ signature in the online application form candidates should check that the images are clear and have been uploaded correctly.** In case the photograph or signature is not prominently visible, the candidate may edit his/ her application and re-upload his/ her photograph or signature, prior to submitting the form. **If the face in the photograph or signature is unclear the candidate's application may be rejected.**

I. GENERAL INFORMATION:

I. Before applying for the post, the applicant should ensure that he/ she fulfils the eligibility and other norms mentioned above for that post as on the specified date and that the particulars furnished by him/ her are correct in all respects.

II. Candidates belonging to reserved category including, for whom no reservation has been mentioned, are free to apply for vacancies announced for General category provided they must fulfil all the eligibility conditions applicable to General category.

III. **In case it is detected at any stage of recruitment that an applicant does not fulfil the eligibility norms and/ or that he/ she has furnished any incorrect/ false information or has suppressed any material fact(s), his/ her candidature will stand cancelled. If any of these shortcomings is/ are detected even after appointment / final selection, his/ her services are/ is liable to be terminated forthwith.**

IV. The applicant should ensure that the application is strictly in accordance with the prescribed format and is properly filled.

V. Appointment of selected candidate is subject to his/ her being declared medically fit as per the requirement of the Bank. Such appointment will also be subject to the service and conduct rules of the Bank for such post in the Bank, in force at the time of joining the Bank.

VI. Candidates are advised to keep their e-mail ID active for receiving communication viz. call letters/ Interview date advice etc., as no communication may be sent in hard copy.

VII. The Bank takes no responsibility for any delay in receipt or loss of any communication whatsoever.

VIII. Candidates serving in Govt./ Quasi Govt. offices, Public Sector undertakings including Nationalized Banks and Financial Institutions are advised to submit **'No Objection Certificate' from their employer at the time of interview**, failing which their candidature shall not be considered and travelling expenses, if any, otherwise admissible, will not be paid.

IX. In case of selection, candidates will be required to produce proper discharge certificate from the employer at the time of taking up the appointment.

X. Candidates are advised in their own interest to apply online well before the closing date and not to wait till the last date to avoid the possibility of disconnection / inability/ failure to log on to the website on account of heavy load on internet or website jam. SBI does not assume any responsibility for the candidates not being able to submit their applications within the last date on account of aforesaid reasons or for any other reason beyond the control of SBI.

XI. DECISION OF BANK IN ALL MATTERS REGARDING ELIGIBILITY, CONDUCT OF INTERVIEW, OTHER TESTS AND SELECTION WOULD BE FINAL AND BINDING ON ALL CANDIDATES. NO REPRESENTATION OR CORRESPONDENCE WILL BE ENTERTAINED BY THE BANK IN THIS REGARD.

XII. The applicant shall be liable for civil/ criminal consequences in case the information submitted in his/ her application are found to be false at a later stage.

XIII. Merely satisfying the eligibility norms does not entitle a candidate to be called for interview. Bank reserves the right to call only the requisite number of candidates for the interview after preliminary screening/ short-listing with reference to candidate's qualification, suitability, experience etc.

XIV. In case of multiple application, only the last valid (completed) application will be retained, the application fee/ intimation charge paid for other registration will stand forfeited.

XV. Any legal proceedings in respect of any matter of claim or dispute arising out of this advertisement and/ or an application in response thereto can be instituted only in Mumbai and Courts/ Tribunals/ Forums at Mumbai alone shall have sole and exclusive jurisdiction to try and entertain any cause/ dispute.

XVI. Outstation candidates, who may be called for interview after short-listing will be reimbursed the cost of travelling by Air fare (Economy Class) for the shortest route in India, maximum up to Rs. 10000/- (total for both sides) OR the actual travel cost in India (whichever is lower) on the basis of actual journey. Local conveyance like taxi/cab/personal vehicle expenses/fares will not be payable / reimbursable. A candidate, if found ineligible for the post will not be permitted to appear for the interview and will not be reimbursed any fare.

XVII. Request for change / correction in any particulars (including category in the application form, once submitted will not be entertained under any circumstances. No correspondence/phone/email will be entertained in this regard. Candidates are advised to fill up the online application carefully and furnish the correct information in this application.

XVIII. **BANK RESERVES RIGHT TO CANCEL / MODIFY THE RECRUITMENT PROCESS EITHER ENTIRELY OR PARTIALLY AT ANY STAGE / TIME FOR ANY PARTICULAR POST / ALL THE POST WITHOUT ASSIGNING ANY REASONS THEREOF, WHATSOEVER.**

XIX. **At the time of interview, the candidate will be required to provide details regarding criminal cases pending against him/her, if any.**
Suppression of material facts will result in cancellation/ termination of candidature at any point, even if the candidate is selected, his/her selection will be canceled in such circumstances. The Bank may also conduct independent verification, inter alia, including verification of Police Records, etc. The Bank reserves the right to deny the appointment depending upon such disclosure and/or independent verification.

For any query, please write to us through link "CONTACT US/ Post Your Query" which is available on Bank's website (https://sbi.bank.in/web/careers/post-your-query)
The Bank is not liable for printing errors, if any.

State bank of India does not endorse, authorize or associate with any external coaching platform, consultancy, individual or digital channel claiming to provide guaranteed selection, influence in recruitment or insider guidance. Candidates must rely solely in information available on SBI's official career portal.

Mumbai
24.02.2026

GENERAL MANAGER (RP&PM)

HOW TO APPLY

Login to https://sbi.bank.in/web/careers/current-openings

Scroll down and click on the respective advertisement.

Download advertisement no. CRPD/SCO/2025-26/25
(Carefully read the detailed advertisement)

Apply Online
(Before final submission, please go through your application.
Corrections will not be allowed after final submission)