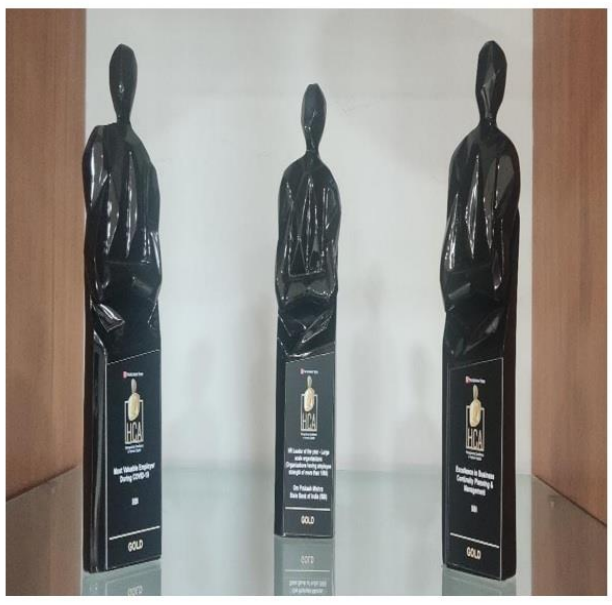
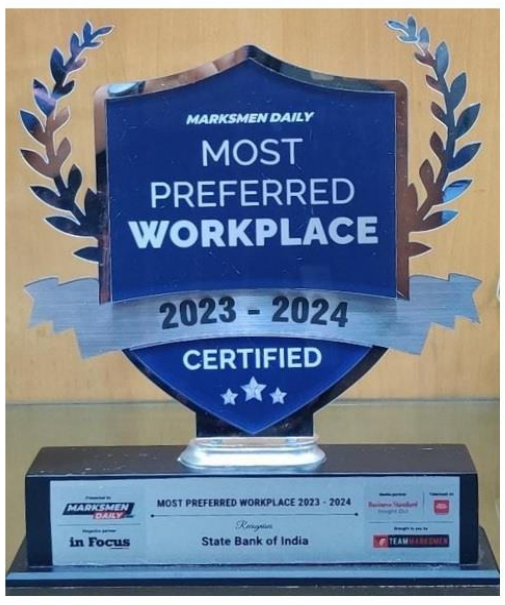
State Bank of India

Central Recruitment & Promotion Department
Corporate Centre, Mumbai
Phone: 022-22820427; Email ID – crpd@sbi.co.in

HR AWARDS & ACCOLADES





ET HUMAN CAPITAL AWARDS

- HR Leader of the Year – Large Scale Organization
- Excellence in Business Continuity Planning & Management
- Most Valuable Employer during COVID 19

MARKSMEN DAILY AWARDS

- Most Preferred Workplace 2023-24

GREENTECH HR AWARDS 2023

- Transformative HR Practices Award
- Employee Engagement Award
- Learning & Development Award
- Compensation & Benefits Award

RECRUITMENT OF SPECIALIST CADRE OFFICERS IN STATE BANK OF INDIA ON REGULAR BASIS
ADVERTISEMENT No. CRPD/SCO/2023-24/32

Online Registration of Application and Online Payment of Fee: From 13.02.2024 To 04.03.2024

State Bank of India invites On-line application from Indian Citizen for appointment in the following Specialist Cadre Officer posts on Regular Basis.
Candidates are requested to apply On-line through the link given in Bank's website https://bank.sbi/web/careers/current-openings or https://sbi.co.in/web/careers/current-openings

1. The process of Registration will be completed only when fee is deposited with the Bank through Online mode on or before the last date for payment of fee.
2. Before applying, candidates are requested to ensure that they fulfill the eligibility criteria for the post as on the date of eligibility.
3. **Candidates are required to upload all required documents (detailed resume, ID proof, age proof, educational qualification (Basic, Other, Additional, Preferred, as the case may be), experience (Mandatory, Compulsory , Other, Additional, Preferred etc.), certificates (wherever issued) evidencing specific skills (Mandatory, Preferred etc.), failing which their candidature will not be considered.**
4. Shortlisting of applications 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). The original documents are mandatorily required for verification before appearing for the interview, if called for.
5. In case a candidate is called for interview and is found not satisfying any / all of the eligibility criteria (Age, Educational Qualification, Category specified Certificate and Experience, etc.) he/ she will neither be allowed to appear for the interview nor be entitled for reimbursement of any travelling expenses.
6. Candidates are advised to check **Bank's website https://bank.sbi/web/careers/current-openings or https://www.sbi.co.in/web/careers/current-openings** regularly for details and updates (including the list of shortlisted/ qualified candidates). Call letter for interview, where required, will be sent by e-mail only **(No hard copy will be sent).**
7. In case more than one candidate scores same marks at 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.
8. **HARD COPY OF APPLICATION & OTHER DOCUMENTS NOT TO BE SENT TO THIS OFFICE.**
9. All revision / corrigenda will be hosted only on the Bank's abovementioned websites.
10. **A CANDIDATE IS PERMITTED TO APPLY FOR MORE THAN ONE POST, IF ELIGIBLE.**

(A) Details of Post: Position / Vacancy / Age/Grade / Place of Posting/Selection Process:

Post No.	Post (Regular)	Grade	Vacancy						PwBD (Horizontal)#				Max. Age@ As on 01.12.2023	Suggested Place of Posting $	Selection Procedure
			SC	ST	OBC	EWS	GEN	Total	VI	HI	LD	d & e			
1	**Assistant Manager (Security Analyst)**	JMGS-I	03	01	05	02	12	**23**	01	--	--	--	30 Years	Mumbai / Navi Mumbai	Shortlisting and Interview
2	**Deputy Manager (Security Analyst)**	MMGS-II	08	03	13	05	22	**51**	01	01	01	--	35 Years		
3	**Manager (Security Analyst)**	MMGS-III	--	--	--	--	03	**03**	01	--	--	--	38 Years		
4	**Assistant General Manager (Application Security)**	SMGS -V	--	--	--	--	03	**03**	01	--	--	--	42 Years		

#PwBD Vacancies are Horizontal and included in total vacancies.
Abbreviations: JMGS-I **–** Junior Management Grade Scale One, MMGS II- Middle Management Grade Scale Two, MMGS III- Middle Management Grade Scale Three, SMGS-V: Senior Management Grade Scale Five.

SC–Scheduled Caste; **ST–**Scheduled Tribe; **OBC–**Other Backward Classes; **EWS**: Economically Weaker Sections; **GEN –** General; **PwBD**-Person with Benchmark Disability; **VI-** Visually Impaired**, HI-** Hearing Impaired**, LD -** Locomotive Disability**, d&e-** Persons with benchmark disabilities under clauses (d) & (e) of section 34 of the Rights of Persons with Disabilities Act 2016

@ Post-1. Not above 30 years as on 01.12.2023 i.e. candidates must have been born not earlier than 02.12.1993.
Post-2. Not above 35 years as on 01.12.2023 i.e. candidates must have been born not earlier than 02.12.1988.
Post-3. Not above 38 years as on 01.12.2023 i.e. candidates must have been born not earlier than 02.12.1985.
Post-4. Not above 42 years as on 01.12.2023 i.e. candidates must have been born not earlier than 02.12.1981.
$: Suggested Place of posting is only indicative, selected candidates may be posted anywhere in India at the sole discretion of the Bank.

RESERVATION FOR PERSONS WITH DISABILITY (PwBD):
4% horizontal reservation has been provided to Persons with Benchmark Disabilities as per section 34 of "Rights of Persons with Disabilities Act, 2016". The post is identified suitable for the Persons with undernoted categories of disabilities as defined in the Schedule of RPWD Act 2016:

Suitable Category of Benchmark Disabilities :	Functional Requirement
a) LV- Low Vision b) D- Deaf, HH-Hard of Hearing c) OA-One Arm, OL-One Leg, CP- Cerebral Palsy, LC-Leprosy Cured, Dw-Dwarfism, AAV-Acid Attacked Victims, d) SLD-Specific Learning Disability, MI-Mental Illness e) MD-Multiple Disabilities involving (a) to (d) above	S- Sitting W- Walking MF- Manipulation by Fingers RW- Reading and Writing SE- Seeing H- Hearing C- Communication

1.	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 'GENERAL' or GENERAL (PwBD) as 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.	Bank reserves the right to cancel the recruitment process entirely or for any particular post at any stage.
4.	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 category candidate should submit OBC certificate containing the **'Non-Creamy Layer'** clause on format prescribed by Govt. of India issued during 01.04.2023 till date of application / online registration valid for the FY.
5.	Reservation for Person with Disability (PwBD) is horizontal within the overall vacancies for the post.
6.	PwBD candidate should produce a certificate issued by a competent authority as per the Govt of India guidelines.

7.	Reservation for Economically Weaker Section (EWS) in recruitment is governed by Office Memorandum no. 36039/1/2019-Estt (Res) dt. 31.01.2019 of Department of Personnel & Training, Ministry of Personnel (DoPT), Public Grievance & Pensions, Government of India. Disclaimer: "EWS vacancies are tentative and subject to further directives of Government of India and outcome of any litigation. The appointment is provisional and is subject to the income & Asset certificate being verified through the proper channels." Benefit of reservation under EWS category can be availed upon production of an "Income & Asset Certificate" issued by a Competent Authority in the format prescribed by Government of India for the Financial Year 2022-23 and valid for the Year 2023-24, based on gross annual income as per DoPT guidelines. The candidate should be in possession of requisite Income and assets certificate in the prescribed format in support of his/ her claim for availing reservation on the date of document verification at the time of interview. If a candidate fails to produce the 'Income & Asset Certificate' in the prescribed format on the date of document verification at the time of interview, he/ she will not be considered for appointment in the Bank for the post.
8.	Maximum age indicated is for General category candidates. Relaxation in upper age limit will be available to reserved category candidates as per Government of India Guidelines.
9.	In cases where experience in a specific field is required, the relevant experience certificate must contain specifically that the candidate had experience in that specific field.
10.	**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.**
11	**In case the certificate of post graduate degree does not specify division and/or percentage marks, the candidate has to produce a certificate from the concerned university/college specifically mentioning the division and / or equivalent percentage marks as the case may be.**
12	**The Experience Certificate to evidence / mention the relevant, required experience for the relevant post (mentioning the requisite nature of duties performed) and the respective period of the same, failing which the candidature will be liable for cancellation.**

(B) Details of Post-wise Educational Qualification / Experience / Specific Skills / Job Profile and KRAs:

1. Assistant Manager (Security Analyst) JMGS-I

Qualifications (As on 01-12-2023)	Post Basic Qualification Experience (As on 01-12-2023)	Specific Skills
Basic:- **Compulsory:** B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology / Electronics / Electronics & Telecommunications / Electronics & Communications / Electronics & Instrumentations OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized university or institution only. **Preferred:** i) M. Tech in Cyber Security / Cyber Forensics / Information Technology ii) CEH / CISA / CISM / CRISK / CISSP / ISO 27001 LA/ VA certifications like GIAC Enterprise Vulnerability Assessor (GEVA)	Candidate having Minimum 2 years' "**post basic qualification"** experience in IT / IT Security / Information Security in Banking, Financial Services and Insurance (BFSI) / Non-Banking Financial Company (NBFC) / Financial Technology (FinTech) / IT MNCs. Note: Training & Teaching experience will not be counted for eligibility. (Post basic qualification experience means : Experience after acquiring the mentioned basic / compulsory qualification. Only this will be counted.)	**Compulsory:** Domain and in-depth technical knowledge of Cyber Security and Security Operations Centre (SOC) and information security operations areas and application security controls and assessments and security monitoring. **Preferred:** Experience in BFSI sector in handling various Information Security roles.

Job Profile and KRAs :

1. Broad knowledge and experience in infrastructure services including Active Directory, Email solutions, Patch Management, Privileged Access Management, IT Asset management etc. Knowledge on authentication and authorization standards applicable in the Web application/ Web services – OAuth2, SAMP, and OpenID.
2. Possess and maintain broad technical and business knowledge of all aspects of Infrastructure security and management technologies including end-point security, mobility management, client operating systems, Sandboxing, Firewall, DLP, VDI, WAF, PAM, Active Directory, Application whitelisting, File Integrity Monitoring, Network Access Control, CDR, infrastructure and endpoint security solutions including Anti-malware, EDR, MDM, Network Access Control, Proxy etc.
3. Implementing software application security controls.
4. Security requirements analysis and implementation for application Threat Modelling, Application Security Test planning & coordination.
5. Participate in Vulnerability Assessment, Penetration, AppSec, Code Review, and Security Configuration reviews.
6. Ability to perform security assessment of web application to identify OWASP Top 10 related vulnerabilities with knowledge of tools like Kali Linux, Burp suite, Nmap, Qualys/Nessus, Metasploit, HCL AppScan etc.
7. Knowledge on widely used Cyber offensive tools & Open-source tools would be an added advantage.
8. Ability to perform security assessment of mobile (Android/iOS) applications to identify OWASP related vulnerabilities with hands-on security testing of mobile applications (Static / Dynamic / Memory Analysis) and experience on Dynamic instrumentation tools like Frida, Magisk etc.
9. Technical knowledge on SOC and security monitoring tools such as SIEM, NBAD, DAM solutions and threat hunting activities.
10. Performing Threat Intelligence activities on a regular basis.
11. Monitor and Manage Threat Intelligence Platform, consume and manage threat feeds, detecting Cyber threats, and alerting and work on cyber threats, indicators of compromise (IoCs), and MITRE, kill chain methodologies.
12. Defining & reviewing rules, policies, algorithms, reports and dashboards as per the audit compliance requirement, operational requirement, threat assessment and application owner's requirement in SBDL / SIEM, UEBA, DAM, NBA, PCAP, TIP, SOAR and Archer.

Remarks: KRA's: KRAs shall be assigned on joining. Job Profile mentioned above are illustrative. Role/Jobs in addition to the above mentioned may be assigned by the Bank from time to time for the above posts.

2. **Deputy Manager (Security Analyst) MMGS-II**

Qualifications (As on 01-12-2023)	Post Basic Qualification Experience (As on 01-12-2023)	Specific Skills
Basic:- B.E. / B. Tech. in Computer Science /Computer Applications/ Information Technology / Electronics /Electronics & Telecommunications / Electronics & Communications / Electronics & Instrumentations from Government recognized university or institution only. **OR** M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized university or institution only. **Preferred:** i) M. Tech in Cyber Security / Cyber Forensics/Information Technology ii) CEH / CISA / CISM / CRISK / CISSP / ISO 27001 LA / VA certifications like GIAC Enterprise Vulnerability Assessor (GEVA) / CISSP / CISM / CEH	**Minimum** 5 years' post basic qualification experience in IT / IT Security / Information Security in Banking, financial services, and insurance (BFSI) / Non-Banking Financial Company (NBFC) / Financial technology (FinTech) / IT MNCs. Training & Teaching experience will not be counted for eligibility. (Post basic qualification experience means : Experience after acquiring the mentioned basic / compulsory qualification. Only this will be counted.)	**Compulsory:** Domain and in-depth technical knowledge of Cyber Security and Security Operations Centre (SOC) and information security operations areas and application security controls and assessments and security monitoring. **Preferred**: Experience in BFSI sector in handling various Information Security roles.

Job Profile and KRAs :

1. Broad knowledge and experience in infrastructure services including Active Directory, Email solutions, Patch Management, Privileged Access Management, IT Asset management etc. Knowledge on authentication and authorization standards applicable in the Web application/ Web services – OAuth2, SAMP, and OpenID.
2. Possess and maintain broad technical and business knowledge of all aspects of Infrastructure security and management technologies including end-point security, mobility management, client operating systems, Sandboxing, Firewall, DLP, VDI, WAF, PAM, Active Directory, Application whitelisting, File Integrity Monitoring, Network Access Control, CDR, Infrastructure and endpoint security solutions including Anti-malware, EDR, MDM, Network Access Control, Proxy etc.
3. Implementing software application security controls.
4. Security requirements analysis and implementation for application Threat Modelling, Application Security Test planning & coordination.
5. Participate in Vulnerability Assessment, Penetration, AppSec, Code Review, and Security Configuration reviews.
6. Ability to perform security assessment of web application to identify OWASP Top 10 related vulnerabilities with knowledge of tools like Kali Linux, Burp suite, Nmap, Qualys / Nessus, Metasploit, HCL AppScan etc.
7. Knowledge on widely used Cyber offensive tools & Open-source tools would be an added advantage.
8. Ability to perform security assessment of mobile (Android / iOS) applications to identify OWASP related vulnerabilities with hands-on security testing of mobile applications (Static/ Dynamic/ Memory Analysis) and experience on Dynamic instrumentation tools like Frida, Magisk etc.
9. Technical knowledge on SOC and security monitoring tools such as SIEM, NBAD, DAM solutions and threat hunting activities.
10. Performing Threat Intelligence activities on a regular basis.
11. Monitor and Manage Threat Intelligence Platform, consume and manage threat feeds, detecting Cyber threats and alerting and work on cyber threats, indicators of compromise (IoCs), and MITRE, kill chain methodologies.
12. Defining & reviewing rules, policies, algorithms, reports and dashboards as per the audit compliance requirement, operational requirement, threat assessment and application owner's requirement in SBDL / SIEM, UEBA, DAM, NBA, PCAP, TIP, SOAR and Archer.
13. Create correlation rules for logs received from disparate IT systems, develop and apply analytical and pattern analysis models on billions of logs received per day by SOC.
14. Create playbooks for automating logs correlation, incident creation, reporting, remediation, escalation & closure verification.
15. Conduct Digital Forensic Analysis using Forensic and Log analysis Tools (Commercial and Open-source tools) such as EnCase, Forensic Toolkits (FTK), ELK, The Sleuth Kit (TSK) etc.
16. Understanding third party-risk and fourth party-risk (Vendor Risk) posed by supply chain, third party vendor and business partner relationship and design, implement and manage core Third Party Risk Management (TPRM) processes to monitor, mitigate and report on risk from third party relationships especially vendors and clients.

Remarks: KRA's: KRAs shall be assigned on joining. Job Profile mentioned above are illustrative. Role/Jobs in addition to the above mentioned may be assigned by the Bank from time to time for the above posts.

3. Manager (Security Analyst) MMGS-III

Qualifications (As on 01-12-2023)	Post Basic Qualification Experience (As on 01-12-2023)	Specific Skills
Basic:- B.E. /B. Tech. in Computer Science /Computer Applications / Information Technology / Electronics / Electronics & Telecommunications / Electronics & Communications / Electronics & Instrumentations from Government recognized university or institution only OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized university or institution only OR MTech in Cyber Security / Information Security from Government recognized university or institution only **Other Qualifications:** **Essential :** CCSP / CCSK / GCSA / CompTIA Cloud+ / VCAP/ CCNA / CCNP **Preferred :** Additional technical certification like CISA/CISM/CISSP/ GSEC CEH	**Minimum** : 7 **years' of Post basic qualification experience** in IT / IT Security / Information Security in Banking, Financial Services and Insurance (BFSI) / Non-Banking Financial Company (NBFC) / Financial technology (FinTech) / IT MNCs (Post basic qualification experience means : Experience after acquiring the mentioned basic / compulsory qualification. Only this will be counted.)	**Essential:** Experience in carrying out Data flow analysis / preparing Data flow diagrams, architecting, recommending, and implementing data security controls as per business objectives and organizational policies. Significant experience with deploying / managing private and public cloud deployments, virtualized environment, and containerization platforms. Proficient with Cloud Security Solutions and Cloud Technologies including CASB / CSPM/ CWPP / CNAPP / Micro segmentation / Virtualization technologies/ containerization technologies. Working experience on providing security recommendations for deployment / management of large Networks. Highly proficient with latest Networking Technologies including Firewall, IPS, Load Balancer, Routers and Switches / Proxy / Anti DDoS / DNS / NAC / AAA / etc. Experience in designing & implementing Network Security solutions like Firewalls, Intrusion Prevention Systems, etc. Responsible for implementing various policies including Information Security Policy, Cyber Security Policy / Data Governance Policy and related procedures and Data Leak prevention solutions. Strong understanding of data classification, data security mechanisms / data protection regulatory requirements, cryptographic techniques. Note: Training & Teaching experience will not be counted for eligibility.

Job Profile and KRAs :

1. Provide advisory role in the selection and design of private and public cloud deployments, virtualization, and containerization technologies such as Azure / AWS / GCP/ VMware Cloud Foundation/ OCI (preferable).
2. Provide expertise in Secure Architecture and recommendations for Cloud deployments, virtualization, and containerization technologies.
3. Develop Cloud Security Policies & Standards and reference Architecture for Cloud adoption.
4. Provide subject matter expertise on information security architecture to application teams.
5. Monitor security posture of Cloud deployments and advise measures to improve them.
6. Possess and maintain broad technical and business knowledge of aspects of Infrastructure technologies including Networking, Authentication Mechanisms and cryptographic controls etc.
7. Carry out Threat Modelling and Risk Analysis.
8. Develop and manage Bank's data security strategy in India, including the development and implementation of Bank's data security policy and procedures.
9. Undertake periodic data security assessments or reviews.
10. Undertake necessary measures to rectify any deficiencies identified by the assessment.
11. Provide advice and assistance for managing data security breaches (if any), including liaising with the Supervisory Authority on behalf of the Bank.

12. Carry out Data flow analysis (DFA) for business and technology departments.
13. Implement the Data Leak prevention (DLP) and Document Rights management solution (IRM / DRM).
14. Provide advisory role in the design of Secure Network Architecture.
15. Develop Security Policies & Standards and reference Architecture for Network design and deployment.
16. Stay abreast of emerging networking technologies, solutions, security threats, vulnerabilities & controls and advise mitigating controls.
17. Review of Network for secure deployments, secure configurations against Global Security Best Practices.
18. Developing network security standards and guiding network design to meet corporate requirements.
19. Monitor security posture of network deployments and advise measures to improve them.
20. Carry out Threat Modelling and Risk Analysis.
21. Conducting network security assessments and monitoring DDoS, WAF, IDS / IPS, Firewall systems.

Remarks: KRA's: KRAs shall be assigned on joining. Job Profile mentioned above are illustrative. Role/Jobs in addition to the above mentioned may be assigned by the Bank from time to time for the above posts.

4. Assistant General Manager (Application Security) SMGS-V

Qualifications (As on 01-12-2023)	Post Basic Qualification Experience (As on 01-12-2023)	Specific Skills
Basic:- BE / BTech (Computer Science / Electronics & Communications / Information Technology/ Cybersecurity) from Government recognized university or institution only OR MCA/ MSc (Computer Science)/ MSc (IT) from Government recognized university or institution only OR MTech in Cyber Security / Information Security from Government recognized university or institution only **Preferred** Additional technical certification out of CISA / CISM / CISSP / GSEC / CompTIA CySA+ / Data+ / SSCP / CCNPSecurity	- 12 plus years' **Post Basic Qualification experience** in information security and Technology professional - Certification in security (CISA, CISM, CISSP) is a strong plus - Prior experience in Threat Modelling, application Security Test planning & coordination, experience in Application risk mitigation planning, Vulnerabilities remediation recommendation & guidance, Compliance & Metrics reporting **-** Advises management on risk issues related to information security and recommend action in support wider risk management and compliance programs. - Monitors information security trends internal / external and keeps leadership informed about information security related trends. - Be aware of various current security solutions, tools and technologies. - Ensure compliance to information security policies and compliance. - Coordinate and submit various CSITE /regulatory submissions. - Monitor compliance with local and industry specific regulations (PCI-DSS, ISO 27001) - Possesses deep understanding of security for cloud computing platforms. (SaaS, PaaS, IaaS) - Drives required risk culture and partnership with peer technology teams and support functions. - Participate in various Security Committee meetings. - Experience in security requirements analysis for application or infrastructure or As TAC resource of an OEM (in the field of Application / Infrastructure security etc.) (Post basic qualification experience means : Experience after acquiring the mentioned basic / compulsory qualification. Only this will be counted.)	**-- --**

Job Profile and KRAs :

1. Providing technical leadership, guidance, and direction on application security
2. Developing and maintaining documentation of application security controls
3. Defining software application security controls.
4. Identifying, Designing and Implementing technical solutions to address security weaknesses.
5. Analysing system services, spotting issues in code, networks and applications
6. Security requirements analysis and implementation for application
7. Threat Modelling, Application Security test planning & coordination
8. Application risk mitigation planning, vulnerabilities remediation recommendation & guidance, compliance & metrics reporting.
9. Knowledge of Threat Modelling / Risk Assessment, Application Risk classification, Security Architecture gap assessment and secure SDLC process definition and tooling.
10. DevSecOps - Security integration in CI/CD pipeline - design, implementation
11. Good knowledge on development aspects and secure coding practices.
12. Responsible for reviewing developed applications, before they are deployed in production environment
13. Carry out comprehensive security reviews of the applications / infrastructure
14. Identify the vulnerabilities that can be exploited by potential malicious hacker
15. Understanding of latest IT security tools / techniques in the application / Infrastructure domains
16. Working with internal and external business partners on ensuring that IT infrastructure / Application meet global security standards.
17. Stay up to date with security news, keeping an eye out for the latest vulnerabilities and remedies emerging in the field.

Remarks: KRA's: KRAs shall be assigned on joining. Job Profile mentioned above are illustrative. Role/Jobs in addition to the above mentioned may be assigned by the Bank from time to time for the above posts.

(C) REMUNERATION:

Post Serial Number	Grade (Regular Position)	Scale of Pay
Assistant Manager (Security Analyst)	JMGS I	Basic Pay: 36000-1490/7-46430-1740/2-49910-1990/7/-63840
Deputy Manager (Security Analyst)	MMGS II	Basic Pay: 48170-1740/1-49910-1990/10-69810
Manager (Security Analyst)	MMGS III	Basic Pay: 63840-1990/5-73790-2220/2-78230
Assistant General Manager (Application Security)	SMGS V	Basic Pay: 89890-2500/2-94890-2730/2-100350
Eligible for DA, HRA, CCA, PF, Contributory Pension Fund i.e., NPS, LFC, Medical Facility etc. as per rules in force from time to time and Salary and perks as per Bank's salary structure.		

(D) SELECTION PROCESS:

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 on the basis of 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.

(E) Call Letter for Interview: Intimation/ call letter for interview will be sent by email / will be uploaded on Bank's website. NO HARD COPY WILL BE SENT.

(F) How to Apply: Candidates should have valid email ID / Mobile phone number which should be kept active till the declaration of result. It will help him/her in getting call letter/ Interview advises etc. by email or over mobile by SMS.

GUIDELINES FOR FILLING ONLINE APPLICATION:

i.	Candidates will be required to register themselves online through the link available on **SBI website https://bank.sbi/web/careers/current-openings OR https://www.sbi.co.in/web/careers/current-openings** and pay the application fee using Internet Banking/ Debit Card/ Credit Card 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 Apply").
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 forms

GUIDELINES FOR PAYMENT OF FEES:

i) Application fees and Intimation Charges (Non-refundable) is Rs 750/- (Seven Hundred Fifty only) for General/ OBC/EWS candidates (Nil for SC/ST/PwBD candidates).
ii) Fee payment will have to be made online through payment gateway available thereat.
iii) 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.
iv) The payment can be made by using Debit Card/ Credit Card/ Internet Banking etc. by providing information as asked on the screen. Transaction charges for online payment, if any, will be borne by the candidates.
v) 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.
vi) If the online payment of fee is not successfully completed in first instance, please make fresh attempts to make online payment.
vii) There is also a provision to reprint the e-Receipt and Application form containing fee details, at later stage.
viii) Application Fee once paid will NEITHER be refunded on any account NOR can it be adjusted for any other examination or selection in future.

(G) How to Upload Documents:

(a) Details of Document to be uploaded:
i. Brief Resume (PDF).
ii. ID Proof (PDF).
iii. Proof of Date of Birth (PDF)
iv. Educational Certificates: Relevant Mark-Sheets/ Degree Certificate (PDF)
v. Experience certificates (PDF)
vi. Caste Certificate/OBC Certificate/EWS Certificate, if applicable (PDF) vii. PwBD Certificate, if applicable (PDF)

(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
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 is 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, number of colours 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. If the Applicant's signature on the answer script, at the time of the examination, does not match the signature on the Call Letter, the applicant will be disqualified.
v. Size of file should be between 10kb - 20kb and Dimensions 140 x 60 pixels.
vi. Ensure that the size of the scanned image is not more than 20kb
vii. Signature in CAPITAL LETTERS shall NOT be accepted.

(d) Document file type/ size:

i. All Documents must be in PDF format.
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 500KB, 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.

(e) Guidelines for scanning of photograph/ signature/ documents:

i. Set the scanner resolution to a minimum of 200 dpi (dots per inch).
ii. Set Colour to True Colour
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 50kb & 20kb 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 other 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 PDF, DOC or DOCX 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.**

Note: In case the face in the photograph or signature is unclear, the candidate's application may be rejected. In case the photograph or signature is not prominently visible, the candidate may edit his/her application and re-load his/ her photograph or signature, prior to submitting the form.

(H) General Information:

i. Before applying for a 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. **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/RECRUITMENT, HIS/ HER SERVICES ARE LIABLE TO BE TERMINATED**.
iii. The applicant should ensure that the application is strictly in accordance with the prescribed format and is properly and completely filled.
iv. Appointment of selected candidate is provisional and 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.
v. Candidates are advised to keep their e-mail ID alive for receiving communication viz. call letters/ Interview date advises etc.
vi. The Bank takes no responsibility for any delay in receipt or loss of any communication.
vii. Candidates belonging to reserved category including, for whom no reservation has been mentioned, are free to apply for vacancies announced for unreserved (General) category provided, they must fulfill all the eligibility conditions applicable to unreserved (General) category. No change in the category of any candidate is permitted after submission of application.
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 may 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/engagement.
x. 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.
xi. 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.
xii. **DECISIONS 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**.
xiii. Multiple applications for the same post are not allowed. In case of multiple applications, only the last valid (completed) application for the intended post will be retained, and the application fee/ intimation charge paid for other registration will stand forfeited. However, a candidate can apply for more than one post, if eligible.
xiv. **Where interview without any written test is the mode of recruitment, merely satisfying the eligibility norms does not entitle a candidate to be called for interview. Bank reserves the right to call only requisite number of candidates for interview after preliminary screening/ short listing with reference to candidate's qualification, suitability, experience etc. The decision of the Bank in this respect shall be final. No correspondence will be entertained in this regard.**
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 only shall have sole and exclusive jurisdiction to try any cause/dispute.
xvi. For the Post serial No. 1., 2. and 3. outstation candidates called for interview will be reimbursed the travel fare of AC-III tier (mail/ express only) for the shortest route in India from the place of present posting / residence whichever is nearer to the interview venue or actual expenses incurred (whichever is lower), on submission of original / copies of tickets / invoice. For the Post serial No.4 i.e. Assistant General Manager (Application Security), Air fare by shortest route Economy class, from place of present posting or residence, whichever is nearer to the interview venue, may be reimbursed on submission of Ticket, Invoice and Boarding Pass. Local transportation expenses will not be reimbursed. A candidate, if found ineligible for the post, will not be permitted to appear in interview and will not be reimbursed any fare.
xvii. At the time of interview, the candidate will be required to provide details regarding criminal case(s) pending against him /her, if any. The Bank may also conduct independent verification, inter alia including verification of police records etc. The Bank reserves right to deny the appointment depending upon such disclosures and/or independent verification.
xviii. **BANK RESERVES RIGHT TO CANCEL THE RECRUITMENT PROCESS ENTIRELY OR FOR ANY PARTICULAR POST AT ANY STAGE**.

For any query, please write to us through link **(CONTACT US/ Post Your Query)** which is available on Bank's website (URL - https://bank.sbi/web/careers OR https://sbi.co.in/web/careers)

CANVASSING IN ANY FORM WILL BE A DISQUALIFICATION

This advertisement is also available on Bank's Website: https://bank.sbi/web/careers/current-openings or https://sbi.co.in/web/careers/current-openings.

The Bank is not responsible for printing errors, if any.

Mumbai - 400021
Dated: 13.02.2024

General Manager (RP&PM)

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

Scroll down and click on advertisement no.

CRPD/SCO/2023-24/32

Download advertisement

(Carefully read the detailed advertisement)

Apply Online

(Before final submission, please go through your application.