STATE BANK OF INDIA

CENTRAL RECRUITMENT & PROMOTION DEPARTMENT
CORPORATE CENTRE, MUMBAI
(Phone: 022-2282 0427; Fax: 022-2282 0411; E-mail: crpd@sbi.co.in)

RECRUITMENT OF SPECIALIST CADRE OFFICERS IN STATE BANK OF INDIA ON REGULAR BASIS
ADVERTISEMENT No. CRPD/SCO-SYSTEM/2019-20/11

1. Online Registration of Application and Online Payment of Fee: From 06.09.2019 To 25.09.2019
2. Date of Online Test (Tentative): 20.10.2019 (only for Post Sl No. 1 to 24)
3. Tentative Date of Downloading Call Letter for Online Test: 10.10.2019 Onwards (only for Post Sl No. 1 to 24)

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/careers** or **https://www.sbi.co.in/careers**

1. A candidate can apply for one post only.
2. The process of Registration is complete only when fee is deposited with the Bank through Online mode on or before the last date for payment of fee.
3. Before applying, candidates are requested to ensure that they fulfill the eligibility criteria for the post as on the date of eligibility.
4. Candidates are required to upload all required documents (brief resume, ID proof, age proof, educational qualification, experience etc.) failing which their candidature will not be considered for short listing/online written test/ interview.
5. Admission to online test/ Short listing will be purely 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).
6. In case a candidate is called for interview and is found not satisfying the eligibility criteria (Age, Educational Qualification and Experience etc.) he/ she will neither be allowed to appear for the interview nor be entitled for reimbursement of any travelling expenses.
7. Candidates are advised to check Bank's website **https://bank.sbi/careers** or **https://www.sbi.co.in/careers** regularly for details and updates (including the list of shortlisted/ qualified candidates). **The Call letter for online Examination and "acquaint yourself" booklet should be downloaded by entering registration number and password/date of birth from the Bank's website. Call letter for interview, where required, will be sent by e-mail only (No hard copy will be sent).**
8. 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.
9. HARD COPY OF APPLICATION & OTHER DOCUMENTS **NOT TO BE SENT TO THIS OFFICE.**
10. **All revision / corrigenda will be hosted only on the Bank's above mentioned websites.**

A. Details of Post (Regular)/Grade/Vacancy/ Age/Selection Process:

Post Sr No.	Post	Grade	Vacancy								Age as on 30.06.2019	Selection Procedure
			GEN	OBC	SC	ST	EWS	Total	PWD		Max	
									LD#	HI		
1	**Developer**	JMGS-I	62	39	22	10	14	147	3	3	30	
2	**Developer**	MMGS-II	16	9	4	2	3	34	1	1	33	
3	**System / Server Administrator**	JMGS-I	21	12	7	3	4	47	1	1	30	
4	**Database Administrator**	JMGS-I	14	7	4	2	2	29	1	1	30	
5	**Cloud Administrator**	JMGS-I	8	3	2	1	1	15	1		30	
6	**Network Engineer**	JMGS-I	8	3	1	1	1	14	1		30	
7	**Tester**	JMGS-I	3	1	–	–	–	4	1		30	
8	**WAS Administrator**	MMGS-II	5	1	–	–	–	6	1		33	
9	**Infrastructure Engineer**	MMGS-II	3	1	–	–	–	4	1		33	
10	**UX Designer**	MMGS-II	3	–	–	–	–	3	1		33	
11	**IT Risk Manager**	MMGS-II	1	–	–	–	–	1	–		33	
12	**IT Security Expert**	MMGS-III	8	3	2	1	1	15	1		38	• Online Written Test & • Interview
13	**Project Manager**	MMGS-III	8	3	1	1	1	14	1		38	
14	**Application Architect**	MMGS-III	4	1	–	–	–	5	1		38	
15	**Technical Lead**	MMGS-III	3	1	–	–	–	4	1		38	
16	**Infrastructure Architect**	MMGS-III	2	–	–	–	–	2	1		38	
17	**Infrastructure Engineer**	JMGS-I	2	–	–	–	–	2	1	–	30	
18	**IT Security Expert**	JMGS-I	27	16	9	4	5	61	3	–	30	
19	**IT Security Expert**	MMGS-II	10	4	2	1	1	18	1	–	35	
20	**IT Risk Manager (IS Dept.)**	MMGS-II	4	1	–	–	–	5	1	–	35	
21	**Infrastructure Architect**	MMGS-II	2	–	–	–	–	2	1	–	35	
22	**Deputy Manager (Cyber Security - Ethical Hacking)**	MMGS-II	6	2	1	–	1	10	1	–	35	
23	**Deputy Manager (Cyber Security - Threat Hunting)**	MMGS-II	3	1	–	–	–	4	1	–	35	
24	**Deputy Manager (Cyber Security - Digital Forensic)**	MMGS-II	3	1	–	–	–	4	1	–	35	
25	**Security Analyst**	MMGS-III	8	3	1	–	1	13	1	–	38	• Short listing & • Interview
26	**Manager (Cyber Security - Ethical Hacking)**	MMGS-III	1	–	–	–	–	1	–	–	38	
27	**Manager (Cyber Security - Digital Forensic)**	MMGS-III	1	–	–	–	–	1	–	–	38	
28	**Chief Manager (Vulnerability Mgmt. & Penetration Testing)**	SMGS-IV	1	–	–	–	–	1	–	–	40	
29	**Chief Manager (Incident Management and Forensics)**	SMGS-IV	2	–	–	–	–	2	1	–	40	
30	**Chief Manager (Security Analytics and Automation)**	SMGS-IV	2	–	–	–	–	2	1	–	40	
31	**Chief Manager (SOC Infrastructure Management)**	SMGS-IV	1	–	–	–	–	1	–	–	40	
32	**Chief Manager (SOC Governance)**	SMGS-IV	1	–	–	–	–	1	–	–	40	
33	**Chief Manager (Cyber Security - Ethical Hacking)**	SMGS-IV	3	–	–	–	–	3	1	–	40	
34	**Chief Manager (Cyber Security - Digital Forensic)**	SMGS-IV	1	–	–	–	–	1	–	–	40	
35	**Chief Manager (Cyber Security - Threat Hunting)**	SMGS-IV	1	–	–	–	–	1	–	–	40	

OA and OL candidates may apply.

ABBREVIATIONS:
Category: GEN- General Category, OBC- Other Backward Class, SC - Scheduled Caste, ST - Scheduled Tribe, EWS-Economically Weaker Section, PWD- Person with Disabilities, LD- Locomotor Disability, OL – One leg Impaired, OA- One Arm Impaired, HI-Hearing Impaired, JMGS- Junior Management Grade Scale, MMGS- Middle Management Grade Scale, SMGS- Senior Management Grade Scale

NOTE:

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 (PWD) 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 at any time.
4. Caste certificate issued by Competent Authority on format prescribed by the Government of India will have to be submitted by the SC/ST candidates.
5. 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 31.03.2019. OBC certificate containing the 'Non-creamy layer' clause, issued during the period 01.04.2019 to the date of interview, should be submitted by such candidates, if called for interview.
6. Reservation for Person with Disability (PWD) is horizontal within the overall vacancies for the post.
7. PWD candidate should produce a certificate issued by a competent authority as per the Govt of India guidelines.
8. Reservation to Economically Weaker Section (EWS) in recruitment is governed by Office Memorandum no. 36039/1/2019-Estt (Res) dated 31.01.2019 of Department of Personnel & Training, Ministry of Personnel, 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 channel."
9. Benefit of reservation under EWS category can be availed upon production of an "Income & Asset Certificate" issued by a Competent Authority on the format prescribed by Government of India.
10. 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.
11. In cases where experience in a specific field is required, the relevant experience certificate must contains specifically that the candidate had experience in that specific field.
12. In cases the certificate of degree/diploma does not specify the field of specialisation, the candidate will have to produce a certificate from the concerned university/college specifically mentioning the specialisation.

(B) Details of Educational Qualification/ Experience/ Likely Place of Posting:

Post Sr No.	Post & Grade	Basic Qualification (Compulsory) as on 30.06.2019	Other Qualification (Compulsory/ Preferred) as on 30.06.2019	Post Basic Qualification Work Experience as on 30.06.2019 (Training & Teaching experience will not be counted for eligibility. (For Post Sl No. 1 to 16, experience should be in "IT sector" & for Post Sl No. 17 to 35, experience should be in "BFSI sector and/or reputed IT companies")
1	Developer (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Experience in Application development (coding, testing and maintenance of application/software). Strong knowledge of .Net/Angular JS/Core JAVA/DB2 SQL - PL SQL/IBM Websphere MQ/J2EE/Oracle 11g/Oracle ADF/PHP/R Programming/ SAP ABAP/Webservice will be preferred.
2	Developer (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Minimum 5 years of post basic qualification experience in Application development (coding, testing and maintenance of application/software). Strong knowledge of .Net/Angular JS/Core JAVA/DB2 SQL - PL SQL/IBM Websphere MQ/J2EE/Oracle 11g/Oracle ADF/PHP/R Programming/SAP ABAP/Webservice.
3	System/Server Administrator (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Experience in IT sector, preferably in System / Server administration post basic qualification will be preferred. **Specific Skill required:** • Strong knowledge of .NET/AIX/IBM • Websphere/LINUX/UNIX Server/MCSA/Oracle • Weblogic/RED HAT/Window Server preferred
4	Database Administrator (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Experience in IT sector preferably in database administration post basic qualification will be preferred. **Specific Skill Required:** • Oracle Certified Professionals • Strong knowledge of DB2 Database/HADOOP/MS SQL Server/Oracle DBA preferred.
5	Cloud Administrator (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Experience in IT sector, preferably in Cloud post basic qualification will be preferred. **Specific Skill Required:** • Strong knowledge in VMWARE ESX/CLOUD COMPUTING preferred.
6	Network Engineer (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Experience in IT sector in handling large corporate network or Banking network post basic qualification will be preferred. • NET/Network Security/Networking Concept/Cisco Certified Network Associate(CCNA) with knowledge of routing, switching protocol, networking devices, sound analytical and troubleshooting skills preferred.
7	Tester (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Experience of IT testing post minimum qualification will be preferred. • Manual Tester/HP Quick Test Professional (Qtp)/Regression Tester preferred.
8	WAS Administrator (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	**Preferred:** CISA and CISM certification	Minimum 5 years of post basic qualification experience in IT business / industry out of which minimum 2 years of extensive experience in managing WAS, HIS, Unix, AIX environments. **Specific Skill Required:** • Familiarity with J2EE, IHS Web Server, WebSphere Application Server, SSL, SOA, Unix Shell, Python and Perl etc. • Unix administration skills on AIX • Familiarity with IBM MQ servers, Oracle / SQL/ DB2 servers and XML, XSL and WSDL. • Familiarity with the Web and Application Servers, Workflow infrastructure. • Some knowledge of business/ organization, Bank standards, infrastructure, architecture and technology in related areas from a design/ support/ solutions perspective. • Is comfortable with working in an environment where a high degree of multitasking is the norm
9	Infrastructure Engineer (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Minimum 5 years of post basic qualification experience in IT sector in installation/ migration / Up-gradation of WebLogic, webserver on Solaris/LINUX/UNIX/AIX etc. **Specific Skill Required:** Experience in installation/ migration / Up-gradation of WebLogic, webserver on Solaris/LINUX/UNIX/AIX etc.
10	UX Designer (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute	-	Minimum 5 years of post basic qualification experience in IT sector in UX design & development/Photoshop/Core Java. **Specific Skill Required:** Experience in UX design & development/Photoshop/Core Java.
11	IT Risk Manager (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute	-	Minimum 5 years of post basic qualification experience in IT sector out of which minimum 2 years' experience in IT Risk Management. **Specific Skill Required:** • Expertise in all aspects of Risk Management including identification, analysis, mitigation, reporting, awareness, Incident Management and Response, GRC, audit and compliance. • Knowledge of risk assessment of Business and IT processes, BCP/DR, projects etc. and developing suitable mitigation plans for the same. • Professional risk /security certification e.g. CRISC, CISSP, CISA, CISM will be preferred. • Knowledge of ISO27001/2, FFIEC and COBIT relevant security frameworks a must • Strong understanding of current regulatory expectations for financial services organizations • Familiarity with infrastructure, networking, security and software development processes • Network & Infrastructure Architecture and Security (including network segmentation concepts, firewalls, routers, VPN solutions etc.) • Systems Development (including SDLC, project management and change control methodologies) • Physical Security & Data Center Environmental Controls • Knowledge of Hosted and Windows environments, Client Server Technology, Networks, Firewalls, SIEM and E-Commerce security risks. • Experience using GRC management applications; experience with RSA-Archer application
12	IT Security Expert (MMGS-III)	Engineering Graduate in Computer Science/IT/ECE or MCA / M.Sc. (IT) / M.Sc. (Computer Science) from recognized University/ Institute.	**Compulsory:** CISA certification	Minimum 8 years of post basic qualification experience in IT out of which minimum 5 years' experience in IT Security. **Specific Skill Required:** • Hands on experience in Risk Assessment, IT Security, IT Production, IT Applications or IT Operations focused Control functions. • Experience in a large corporation/BFSI preferred

13	Project Manager (MMGS-III)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	**Compulsory:** Certification from PMI. **Preferred:** MBA from reputed institute	Minimum 8 years of post basic qualification experience in IT business/industry out of which minimum 5 years in Building and Leading high-performing, agile team focused on planning, development strategies/initiatives and product lifecycle/service orientation post minimum qualification. **Specific Skill Required:** Experience in Building and Leading high-performing, agile team focused on planning, development strategies/initiatives and product lifecycle/service orientation.
14	Application Architect (MMGS-III)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Minimum 8 years of post basic qualification experience in IT business / industry out of which minimum 3 years' experience as Application and Middleware Architect in E-channels (eg: INB, ATM, Mobile etc.). **Specific Skill Required:** • Experience as Application and Middleware Architect in E-channels (eg: INB, ATM, Mobile etc.). • Experience in AGILE Methodology/Core JAVA/IBM Websphere MQ/LINUX/UNIX Server preferred
15	Technical Lead (MMGS-III)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Minimum 8 years of post basic qualification experience in IT Business/Industry in development, testing and support of Mobile or e-channel software development lifecycle. **Specific Skill Required:** • Experience in in development, testing and support of Mobile or e-channel software development lifecycle. • Strong knowledge of Scrum/Cloud Computing/Jenkins
16	Infrastructure Architect (MMGS-III)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Minimum 8 years of post basic qualification experience in designing and building large IT infrastructure projects. **Specific Skill Required:** • Experience in in designing and building large IT infrastructure projects encompassing both Hardware, Virtualization and middleware layers • Candidates with Professional certifications on OS (Unix), Middleware, Storage, Load Balancer are preferred
17	Infrastructure Engineer (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Experience in IT sector in installation/ migration / Up-gradation of WebLogic, webserver on Solaris/LINUX/UNIX/AIX etc. post minimum qualification will be preferred.
18	IT Security Expert (JMGS-I)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	**Preferred:** • CISSP/CISM/CISA Certification	Experience in IT sector out of which 2 years' experience in IT Security will be preferred. **Specific Skill Required:** • Hands on experience in Risk Assessment, IT Security, IT Production, IT Applications or IT Operations focused Control functions. • Experience in a large corporation/BFSI preferred.
19	IT Security Expert (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	**Preferred:** • CISSP/CISM/CISA Certification.	Minimum 5 years' of post basic qualification experience in IT sector out of which minimum 2 years' experience in IT Security. **Specific Skill Required:** • Hands on experience in Risk Assessment, IT Security, IT Production, IT Applications or IT Operations focused Control functions. • Experience in a large corporation/BFSI preferred.
20	IT Risk Manager (IS Dept.) (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Minimum 5 years' of post basic qualification experience in IT sector out of which minimum 2 years' experience in IT Risk Management. **Specific Skill Required:** • Expertise in all aspects of Risk Management including identification, analysis, mitigation, reporting, awareness, Incident Management and Response, GRC, audit and compliance. • Knowledge of risk assessment of Business and IT processes, BCP/DR, projects etc. and developing suitable mitigation plans for the same. • Professional risk /security certification e.g. CRISC, CISSP, CISA, CISM will be preferred. • Knowledge of ISO27001/2, FFIEC and COBIT relevant security frameworks a must • Strong understanding of current regulatory expectations for financial services organizations • Familiarity with infrastructure, networking, security and software development processes • Network & Infrastructure Architecture and Security (including network segmentation concepts, firewalls, routers, VPN solutions etc.) • Systems Development (including SDLC, project management and change control methodologies • Physical Security & Data Center Environmental Controls • Knowledge of Hosted and Windows environments, Client Server Technology, Networks, Firewalls, SIEM and E-Commerce security risks. • Experience using GRC management applications; experience with RSA-Archer application
21	Infrastructure Architect (MMGS-II)	Engineering Graduate in Computer Science/IT/ECE or MCA/ M.Sc.(IT) / M.Sc. (Computer Science) from recognized University/ Institute.	-	Minimum 5 years of post basic qualification experience in designing and building large IT infrastructure projects. **Specific Skill Required:** • Experience in designing and building large IT infrastructure projects encompassing both Hardware, Virtualization and middleware layers • Candidates with Professional certifications on OS (Unix), Middleware, Storage, Load Balancer are preferred.
22	Deputy Manager (Cyber Security - Ethical Hacking) (MMGS-II)	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	**Compulsory**: Certified Ethical Hacker(CEH) **Preferred**: SANS GIAC certifications / Offensive Security certified Professional (OSCP) / EC-Council Certified Security Analyst (ECSA) / Licensed Penetration Tester (LPT)	Minimum 5 years' post basic qualification experience in Cyber Security. Out of 5 years of experience, minimum three (3) years in Ethical Hacking / Application or Mobile Security Testing/ Red Team exercises. **Specific Skill Required:** • Experience in Web Application Security Testing, Mobile App security testing, Network, System and Application vulnerability assessment & penetration testing, ICS/ IoT device security testing and Red Team exercises. • Extensive experience in addressing web application security issues, such as those outlined in OWASP Top 10 attacks. • Strong knowledge of application security throughout the software lifecycle and DevSecOps • Experience in working with common application, network security tools such as Open source or commercial testing tools like Kali Linux, Metasploit, Burp Suite, Fortify, AppScan, WebInspect etc. • Using various scripting languages such as Python, Perl, Bash, etc. • Excellent verbal, analytical and written communication skills.
23	Deputy Manager (Cyber Security - Threat Hunting) (MMGS-II)	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	**Preferred:** Certified Threat Intelligence Analyst (CTIA) / SANS GIAC certification on incident response and threat hunting areas / Certified Information Systems Security Professional (CISSP)	Minimum 5 years' post basic qualification experience in Cyber Security. Out of 5 years of experience, minimum two (2) years in Threat Hunting / Malware analysis and reverse engineering. **Specific Skill Required:** • Performing Threat hunting on a regular basis • Perform reverse engineering on malware as required to facilitate investigation and analysis • Characterize suspicious binaries and be able identify traits, C2, and develop network and host-based IOCs. • Identify potential malicious activity from memory dumps, logs, and packet captures. • Writing Scripting for threat hunting. • Excellent verbal, analytical and written communication skills.

24	Deputy Manager (Cyber Security - Digital Forensic) (MMGS-II)	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	**Compulsory:** Computer hacking forensic investigator(CHFI) from EC-Council / Encase Certified Examiner (EnCE) **Preferred:** Certified Threat Intelligence Analyst (CTIA) / SANS GIAC certification on incident response and threat hunting areas / Certified Information Systems Security Professional (CISSP)	Minimum 5 years post basic qualification experience in Cyber Security. Out of 5 years of experience, minimum three years in Digital forensic analysis. **Specific Skill Required:** • Experience in Digital Forensic Analysis and Forensic Tools (Commercial and Open source tools) such as EnCase, Forensic Toolkits (FTK) etc. • Conduct Forensic examination of digital and other evidences and should be able to analyze the incidents for forensic investigations. • Strong technical Knowledge on security of network, systems, applications, mobile apps etc. • Excellent verbal, analytical and written communication skills.
25	Security Analyst (MMGS-III)	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	**Compulsory**: • CEH **Preferred**: • CISSP / CISA / CISM • SOC security technology certification from OEM like SIEM/UEBA/SOAR/VM/DAM/PCAP/NBA	• Minimum 7 years post basic qualification experience in IT / IT Security / Information Security. Out of which minimum 2 years in SOC operations. • Experience on Security Technology & Solutions: (At least one is Mandatory) • SIEM – Event Analysis, Rule creation, automation, Asset Integration • Vulnerability Management and penetration testing, OWASP Vulnerabilities and application security risks • User & Network Behaviour Analysis, packet-capture and packet flows analysis • Database Activity Monitoring, security policy creations and database integrations. • Thorough understanding of logs decoding / parsing & correlation techniques, correlation cross-IT technologies logs, deployment methods of above SOC technologies, sub-components of SOC technologies, dash-boarding, ingestion of logs from SOC technologies into each other for 360 degree correlation, threat hunting for IOCs and leveraging threat intelligence, data mining etc. • Understanding of IT Infrastructure technologies and architecture to utilize the same for SOC fine-tuning • Understanding of IT Security technologies like Firewalls, IPS, WAF, AV, AD, DLP, LB, PIMS, ITAM, IAM, RASP, VPN, EDR, Anti-APT and networking protocols & technologies like routers, switches, SDN to utilize same for logs correlation • Understanding of emerging technologies like AI/ML, blockchain, RPA, IOT, Cloud • Digital Forensic Investigation • System admin knowledge (Windows/Linux) • Programming knowledge – Python/ Perl/shell/PHP
26	Manager (Cyber Security - Ethical Hacking) (MMGS-III)	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	**Compulsory**: Offensive Security Certified Professional (OSCP) / Certified Information Systems Security Professional (CISSP) / SANS GIAC certifications on Application / Mobile / Network Security Assessment or Testing areas **Preferred**: Offensive Security certified Expert (OSCE) / EC-Council Certified Security Analyst (ECSA) / Licensed Penetration Tester (LPT)	Minimum 7 years post basic qualification experience in Cyber Security. Out of the 7 years of experience , minimum three (3) years in Ethical Hacking / Application or Mobile Security Testing/ Red Team exercises **Specific Skill Required:** • Experience in Web Application Security Testing, Mobile App security testing, Network, System and Application vulnerability assessment & penetration testing, ICS/IoT device security testing. • Extensive experience in addressing web application security issues, such as those outlined in OWASP Top 10 • Strong knowledge of application security throughout the software lifecycle and DevSecOps • Experience in working with common application, network security tools such as Open source or commercial testing tools like Kali Linux, Metasploit, Burp Suite, Fortify, AppScan, WebInspect etc. • Using various scripting languages such as Python, Perl, Bash, etc. • Strong background in the information and cyber security domain with deep subject matter expertise / knowledge. • Experience of enterprise security architecture and information / cyber security areas such as identify and Access Management, Data Protection , Vulnerability Management ,application security, infrastructure security, and Security Monitoring and Response. • Up-to-date with key regulation / developments in Information and Cyber Security • Excellent verbal, analytical and written communication skills.
27	Manager (Cyber Security - Digital Forensic) (MMGS-III)	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	**Compulsory**: Computer hacking forensic investigator(CHFI) from EC-Council / Encase Certified Examiner (EnCE)/ SANS GIAC certification on Digital Forensics / SANS GIAC certification on incident response area **Preferred**: Certified Information Systems Security Professional (CISSP)	Minimum 7 years post basic qualification experience in Cyber Security. Out of 7 years of experience, minimum three (3) years in Digital forensic analysis. **Specific Skill Required:** • Experience in Digital Forensic Analysis and Forensic Tools (Commercial and Open source tools) such as EnCase, Forensic Toolkits (FTK) etc. • Conduct Forensic examination of digital and other evidences and should be able to analyse the incidents for forensic investigations. • Strong technical Knowledge on security of network, systems, applications, mobile apps etc. • Excellent verbal, analytical and written communication skills.
28	Chief Manager (Vulnerability Mgmt. & Penetration Testing) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory**: CVA/ CPT **Preferred:** CPEN / OSCP / CISM / CISSP / CRISC / GPEN Certification SOC security technology certification from OEM like VM, DAM, SIEM	• Minimum 9 years post basic qualification experience in IT and IT / Information Security. Out of 9 years of experience, minimum 5 years experience should be in Vulnerability Management & Penetration Testing areas. • Strong experience in conducting surface, intrusive and offensive external and internal security testing like vulnerability assessment, penetration testing, application security testing, code review and security configuration verification. • Deep Vulnerability assessment and penetration testing skills on IT infrastructure, web applications, Mobile platforms and cloud platforms, based on global security testing practices, frameworks and methodologies. • Hands on experience on commercial, open source security testing and analysis tools (Kali, Metasploit, Burp Suite, Wireshark, Webinspect, HP fortify, Nmap etc.) and common vulnerability scanning tools (Qualys, Nessus, AppScan, etc.). • Strong knowledge of common vulnerability frameworks (CVSS, OWASP), NVD & CVEs. • Scripting knowledge: Python/Perl/Shell/Bash. • Strong Knowledge of Infrastructure Architecture Design, Networking & software Architecture, security and networking protocols • Well versed with system, application, and database hardening techniques and best practices • Experience in performing web application security assessments using hands on techniques for identifying OWASP top 10 vulnerabilities such as XSS, SQL injections, CSRF etc. **Preferred Skills**: • Experience in handling vulnerabilities in digital & cyber ecosystem, social ecosystem platform, platforms like blockchain, AI/ML, IOT, Cloud etc. • Experience in Red & Blue teaming activities & Email Phishing attack simulators / tools. • Analytical and Communication skills

29	Chief Manager (Incident Management and Forensics) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory:** • Computer hacking forensic investigator(CHFI) from EC-Council / Encase Certified Examiner (EnCE)/ SANS GIAC certification on Digital Forensics / SANS GIAC certification on incident response area **Preferred:** • ECIH /GCIH / CISSP / CRISC / CISA / CISM Certification • SOC security technology certification from OEM like DAM, SIEM, UEBA, SOAR	• Minimum 9 years post basic qualification experience in IT/ Information Security. Out of 9 years of experience, minimum 5 years' experience in SOC emanating incident management and Forensics & analysis. • Work experience on various SIEM / UEBA / DAM / SOAR / NBA / PCAP platforms and incident management tools • Well acquainted with ISO 27035, NIST, ITIL and COBIT frameworks. • Hands on experience in Incident Management Life Cycle in IT and Information Security. • Strong technological and processes knowledge on cyber-attack kill chain including Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection Command and Control, Exfiltration etc. • Deep experience in Cyber Security Incident Response including incident analysis, recovery and impact analysis. • Hands on experience on integration of IT assets with SOC, correlation and analysis of logs of different assets like firewalls, IPS, WAF, OS, RDBMS, DLP, AD, AV, Load Balancers, ITAM, PIMS, IAM etc. • Work experience on various SIEM/ UEBA/ DAM/ SOAR platforms and incident management tools • Strong Knowledge of Infrastructure Architecture Design, Networking & software Architecture, Windows and UNIX operating systems, security and networking protocols • Deep understanding of emerging technologies and corresponding security threats. **Preferred skills:** • Experience in various IT security solutions such as Antivirus, DLP, WAF, IDS/IPS, PIMS, Anti-Apt, EDR Solutions etc. • Experience in Next Gen SOC technologies like UEBA, SOAR, Secure Big Data Lake, Threat Intel Platforms, Red & Blue Teaming tools. • Analytical and Communication skills.
30	Chief Manager (Security Analytics and Automation) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory:** • CISSP **Preferred:** • CRISC / CISA / CISM Certification • SOC security technology certification from OEM like DAM, SIEM, UEBA, SOAR is preferred	• Minimum 9 years post basic qualification experience in IT/ IT Security / Information Security. Out of 9 years of experience, minimum 5 years in automation & security Analytics. • Scripting knowledge: Python/Perl/Shell/Bash. • API integration with various IT and SOC systems. • various SIEM/UEBA/Security Big Data Lake, SOAR platforms and incident management tools • Various frameworks of Robotic Process Automation (RPA), Machine Learning, pattern analysis and Modeling in SOC / information security domain. • Designing and customizing security incident playbooks. • Customization and automating day to day manual operations such as automation of analytics workflows, incident remediation/responses, operationalization of threat intelligence etc. • Security analytics tools and technologies to Integrate and correlate disparate data sets. • Correlating and contextualizing security data using the output from 2 or more tools & technologies • Creation of runbooks and mapping them to Incident Response workflows • Automation & orchestration platforms, deployment of AI/ML technologies for security analytics. • Deep understanding of emerging technologies like blockchain, IOT, AI/ML etc. and corresponding security threats **Preferred skills**: • Open source analytical tools.
31	Chief Manager (SOC Infrastructure Management) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory:** • CISSP / ITIL Expert / Certified Lead Implementer Professional **Preferred:** • ISO 27001 Lead Auditor Certification	• Minimum 9 years post basic qualification experience in IT/ IT Security / Information Security. Out of 9 years of experience, minimum 5 years in managing end to end IT infrastructure.. • Strong experience in SOC infra management • Understanding of SOC technologies like SIEM, UEBA, SOAR, DAM, VM, Threat intelligence and services like Anti-phishing, External Penetration Testing. • Implementation of secured configuration of settings / hardening, closure of vulnerabilities by implementing patches, upgradation of version in SOC Infra setup • Installation of OS, applications, RDBMS, web servers, open source technologies and configure them as per corporate requirements • Integration of It Infrastructure with PIMS, IAM, SSO, AD, AV, ITAM, ITSM, DLP, NAC • Security of IT Infrastructure by deploying security technologies like firewalls, IPS, WAF etc. • Uptime management, manage LAN and integration with corporate network, • Credential / user management, roles and groups management, undertake administrative activities on IT / SOC infrastructure • IT Infra related SLA management with multiple vendors & OEMs • Developing Business Continuity and DR Plan • Implementation of encryption, hashing techniques for secured communication, processing and storage of data • Understanding core IT architecture principles like client-server applications, multi-tier web applications, relational & Non-relational databases, firewalls, VPNs, IPS • Understanding of commonly used internet and networking protocols TCP/IP, SMTP, HTTP, FTP, SNMP, POP, LDAP etc. • IT Infrastructure management, cloud management • Roll out of patches, bug fixes on IT Infra, backup and recovery, user access management, integration of IT assets with various IT security technologies like PIMS, IAM, AD, AV, ITSM, ITAM etc. **Preferred skills:** • Setting up or managing private cloud or any multitenant clouds for SOC. • Setting up or managing big data lake or security big data lake. • Experience in various IT security solutions such as Antivirus, DLP, WAF, IDS/IPS, PIMS, Anti-Apt, EDR Solutions etc.
32	Chief Manager (SOC Governance) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory:** • CISA **Preferred:** • CISSP/ ISO 27001 Lead Auditor Certification	• Minimum 9 years post basic qualification experience in IT / IT Security / Information Security. Out of 9 years of experience, minimum 5 years in SOC/Information security Governance. • Strong experience in IT / SOC Governance • Well acquainted with ISO 27001/27002, NIST, ITIL and COBIT frameworks. • Understanding of SOC technologies like SIEM, UEBA, SOAR, DAM, VM, Threat intelligence and services like Anti-phishing, External Penetration Testing. • Implementation of Information Security Policy and Procedures, SOPs in SOC or similar establishment • Hands on experience in implementing / auditing ISO 27001 ISMS standards • Hands on experience on aligning IT / Information security operations with NIST for Identify, Protect, Detect, Respond and Recover areas. • thorough understanding of patch, version, user access and change management strategies and techniques, segregation of duties, shift management • various domestic and global statutory and regulatory reporting • Developing Business Continuity and DR Plan • Understanding core IT architecture principles like client-server applications, multi-tier web applications, relational & Non-Relational databases, firewalls, VPNs, IPS • Understanding of commonly used internet and networking protocols TCP/IP, SMTP, HTTP, FTP, SNMP, POP, LDAP etc. **Preferred skills:** • Deep understanding of domestic and foreign data security laws and their implementation, COBIT, NIST, HIPAA, PCI DSS, encryption methods etc.

33	Chief Manager (Cyber Security - Ethical Hacking) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory:** Offensive Security Certified Professional (OSCP) / Certified Information Systems Security Professional (CISSP) / SANS GIAC certifications on Application / Mobile / Network Security Assessment or Testing area **Preferred:** Offensive Security certified Expert (OSCE) / EC-Council Certified Security Analyst (ECSA) / Licensed Penetration Tester (LPT)	Minimum 9 (Nine) years post basic qualification experience in Cyber Security. Out of 9 years of experience, minimum 5 years in Ethical Hacking / Application or Mobile Security Testing/ Red Team exercises. **Specific Skill Required:** • Experience in Web Application Security Testing, Mobile App security testing, Network, System and Application vulnerability assessment & penetration testing, ICS/IoT device security testing, Red Team exercises. • Extensive experience in addressing web application security issues, such as those outlined in OWASP Top 10 • Strong knowledge of application security throughout the software lifecycle and DevSecOps • Experience in working with common application, network security tools such as Open source or commercial testing tools like Kali Linux, Metasploit, Burp Suite, Fortify, AppScan, WebInspect etc. • Using various scripting languages such as Python, Perl, Bash, etc. • Strong background in the information and cyber security domain with deep subject matter expertise / knowledge. • Experience in Security Code reviews. • Excellent verbal, analytical and written communication skills.
34	Chief Manager (Cyber Security - Digital Forensic) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory:** Computer hacking forensic investigator(CHFI) from EC-Council / Encase Certified Examiner (EnCE)/ SANS GIAC certification on Digital Forensics / SANS GIAC certification on incident response area **Preferred:** Certified Information Systems Security Professional (CISSP)	Minimum 9 (Nine) years post basic qualification experience in Cyber Security. Out of 9 years of experience, minimum 5 years in Digital forensic analysis. **Specific Skill Required:** • Experience in Digital Forensic Analysis and Forensic Tools (Commercial and Open source Tools) such as EnCase, Forensic Toolkits (FTK) etc. • Conduct Forensic examination of Digital and other evidences and should be able to analyse the incidents for Forensic investigations. • Strong technical Knowledge on security of network, systems, applications, mobile apps etc. • Experience of threat hunting, Indicators of Compromise (IOC) Analysis and Malware Analysis and reverse engineering. • Experience in Digital Forensic analysis. • Excellent verbal, analytical and written communication skills.
35	Chief Manager (Cyber Security - Threat Hunting) (SMGS-IV)	B.E. / B. Tech. in Computer Science / Computer Applications / Information Technology OR M.Sc. (Computer Science) / M.Sc. (IT) / MCA from Government recognized University or institution	**Compulsory:** Certified Threat Intelligence Analyst (CTIA) / SANS GIAC certification on incident response and threat hunting areas **Preferred:** Certified Information Systems Security Professional (CISSP)	Minimum 9 (Nine) years post basic qualification experience in Cyber Security. Out of 9 years of experience, minimum 3 years in Threat Hunting / Malware analysis and reverse engineering. **Specific Skill Required:** • Performing Threat hunting on a regular basis • Perform reverse engineering on malware as required to facilitate investigation and Analysis • Characterize suspicious binaries and be able identify traits, C2, and develop network and host-based IOCs. • identify potential malicious activity from memory dumps, logs, and packet captures. • Writing Scripting for Threat hunting. • Excellent verbal, analytical and written communication skills. • Experience of Threat hunting, Indicators of Compromise (IOC) Analysis and malware Analysis and reverse engineering. • Excellent verbal, analytical and written communication skills.

For Post Sl No. 1 to 16, experience should be in "IT Sector" & for Post Sl No. 17 to 35, experience should be in "BFSI sector and/or reputed IT companies".
Place of Posting: Mumbai / Navi Mumbai (depends on the post). The place of posting is only indicative. The selected candidate may be posted anywhere in India.

C. Job Profile & KRAs:

Post Sr No	Post & Grade	Job Profile & KRA in Brief
1	Developer (JMGS-I)	• Carry out developments • Identify and evaluate different IT-related potentials in relation to business needs • Ensure usability and performance of the solution • Participate in efforts to drive development of the systems area • Develop solutions designed to maximize business value • Able to rapidly acquire knowledge of a given domain • Challenge prevailing solutions and assumptions • Effective in ensuring that deliverables are in conformance with system architecture and standards for development • Contribute actively to realization of the business unit's mission and vision • Cope efficiently with multiple assignments and delivers a high standard • Communicate efficiently and purposefully with internal customers and business partners • Demonstrate flexibility and adaptability as required by circumstances • Actively assist in developing others through, e.g. communicating knowledge and participating in professional networks • Maintain focus on the quality of own work e.g. by taking unit tests
2	Developer (MMGS-II)	• Carry out developments • Identify and evaluate different IT-related potentials in relation to business needs • Ensure usability and performance of the solution • Participate in efforts to drive development of the systems area • Develop solutions designed to maximize business value • Able to rapidly acquire knowledge of a given domain • Challenge prevailing solutions and assumptions • Effective in ensuring that deliverables are in conformance with system architecture and standards for development • Contribute actively to realization of the business unit's mission and vision • Cope efficiently with multiple assignments and delivers a high standard • Communicate efficiently and purposefully with internal customers and business partners • Demonstrate flexibility and adaptability as required by circumstances • Actively assist in developing others through, e.g. communicating knowledge and participating in professional networks • Maintain focus on the quality of own work e.g. by taking unit tests
3	System/Server Administrator (JMGS-I)	• System / server installation, configuration and monitoring. • Responsible for the installation, support and maintenance of a computer system/server/storage/network. • Patch updation/upgradation and migration. • Design new computer systems system and server performance • Avoiding server downtime through scheduled maintenance, ensuring server security, and assisting staff in connecting to the server. • System performance monitoring and improvement. • Optimize processes and lead process improvement • Manage staff and user credentials and frameworks • Troubleshoot technical issues • Create and implement training for staff • Coordinate and provide support for Firewall and network system installation/configuration • System/server/network security monitoring and capacity planning. • Risk mitigation planning • DC/DR server configuration set-up and maintenance
4	Database Administrator (JMGS-I)	• Software installation, configuration and Maintenance: L To collaborate on the initial installation and configuration of a new Oracle, SQL Server etc. L To set up hardware and deploys the operating system for the database server. L To transfer data from the existing system to the new platform/data migration • Data Extraction, Transformation, and Loading: Efficiently importing large volumes of data that have been extracted from multiple systems into a data warehouse environment. • Specialized Data Handling: Managing a very large database (VLDB) may require higher-level skills and additional monitoring and tuning to maintain efficiency. • Database Backup and Recovery: L To create backup and recovery plans and procedures based on industry best practices L Backup of cost, time & money and persuade management to take necessary precautions to preserve data. • Security: Implementing and monitoring best practices to minimize risks. • Authentication: Setting up employee access is an important aspect of database security. (control who has access and what type of access they are allowed) • Capacity Planning • Performance Monitoring: Monitoring databases for performance issues & making configuration changes to the software or add additional hardware capacity • Database Tuning: Proactively tune a system based on application and usage instead of waiting until a problem develops. • Troubleshooting: Quickly understand and respond to problems when they occur. • DC/DR server configuration set-up, maintenance and capacity planning.

5	Cloud Administrator (JMGS-I)	• Setting, configuration and maintenance of Bank's Cloud environment. • Virtual Branch complaint management • DC/DR set up for cloud platform. • Set pricing for the catalogue items • Define and activate provisioning rules • Define and activate tagging rules • Define change control parameters for cloud resources • Customize the user experience: Provisioning rules and UI policies • Define the schedule for downloading billing data • Approve change requests associated with modifications to cloud resource • View pending approvals for cloud resources • View and analyse summary data on cloud resource deployments • Monitor requests and key metrics for cloud resources • Deadlock prevention and detection • Debugging issues • Managing and monitoring SQL jobs , data export and import , database replication, encryption , ELB, EBS, S3, CloudFront, Aurora • Maintaining IIS, Apache, PHP sites, .Net sites, FTP sites, SMTP , Linux servers, backup, restore, multiple VPN • Optimizing queries, table structure, indexing • Setup secure environment according to client/project requirements • Capacity planning.
6	Network Engineer (JMGS-I)	• Network devices installation and capacity planning. • Establish networking environment by designing system configuration; directing system installation; defining, documenting, and enforcing system standards • Maximize network performance by monitoring performance; troubleshooting network problems and outages; scheduling upgrades; collaborating with network architects on network optimization • Secure network system by establishing and enforcing policies; defining and monitoring access • Update job knowledge by participating in educational opportunities; reading professional publications; maintaining personal networks; participating in professional organizations • Accomplish information systems and organization mission by completing related results as needed • Reporting network operational status by gathering, prioritizing information; managing projects • Skills: Tracking Budget Expenses, Project Management, Problem Solving, LAN Knowledge, Proxy Servers, Networking Knowledge, Network Design and Implementation, Network Troubleshooting, Network Hardware Configuration, Network Performance Tuning,
7	Tester (JMGS-I)	• Define test scripts and cases • Execution of test scripts/cases • Ongoing improvements in test scripts and maintenance of reports of test cases. • White-box, Grey-Box and Black-box testing • Documenting test results • Ensure that a detailed test scripts/cases, scenarios and instructions are available prior to the start of testing • Ensure that issues identified during UAT are logged in the Test Log • Ensure testing takes place within agreed timeframes • Understanding of business requirements and functional specification documents • Assistance in defect classification and Reporting • Provision of data required for preparation of status reports • Good understanding of Automation Test Tool • Updation of daily activities in Daily Status Report at the end of day
8	WAS Administrator (MMGS-II)	• WAS installation, configuration and maintenance • Supporting large scale WAS infrastructures with multiple middle ware products • Setting up, configuring and troubleshooting WAS & IHS in AIX • Setting up SSL configuration, Load balancer • Setting up J2EE, IHS Web Server, WebSphere Application Server, SSL, SOA, Unix Shell, Python and Perl etc. • Setting up IBM MQ servers, Oracle / SQL/ DB2 servers and XML, XSL and WSDL • Setting up Web and Application Servers, Workflow infrastructure and trouble shooting • Performance tuning and improvements • Capacity planning
9	Infrastructure Engineer (MMGS-II)	• Installation/ migration/ Up-gradation of WebLogic on Solaris/LINUX/UNIX • Sizing, capacity planning, evaluation and procurement of hardware. • Installation of new equipment, hardware swap-outs and component replacements (servers, network equipment and storage) • Implementation of virtualization. • Installation and maintenance of electrical supplies and equipment. Installation of associated infrastructure such as network patching • Network cabling and testing • Supplier liaison - arranging orders and deliveries with infrastructure vendors • Experience of web application deployment on WebLogic using console & command line • Integration of web servers/application servers and DB servers. • Management of SSL certs on webservers / app servers • Troubleshooting of logs, providing logs on demand from different teams (Architects, developers and validations) • Providing thread /heap dump as per requirement • Working with different teams during production deployment Automation of the tasks using shell scripting • Ensure periodic health checks and take appropriate steps for high availability • Ensure that predefined SLA is maintained • Ensure that 100% BCP is provisioned in all respect • Responsible for implementation of ITIL/ITSM tools (Minimal Manual intervention) • Regular interaction with IT Partners on the Infra roadmap and put up reports to all stake holders • Responsible for Patch Management as per Bank's IT/IS Policy • Regular communication with application owners on above matters • Ensure documentation of entire architecture design and evaluation work • Migration to new systems, capacity planning, performance monitoring and improvement.
10	UX Designer (MMGS-II)	• Study industry best-practices in UX design • Designing Wireframe websites and mobile apps • Work closely with internal design and programming team to collate content and program manage the development of the website • Work closely with the product team to identify users' needs and understand how users consume and navigate content • Carry out an assessment of existing information architecture and identify areas for improvement, including content inventories and audits • Plan and design the information architecture for the website or applications • Create use cases and flow diagrams, and define information hierarchies • Labelling of information • Create wireframes and taxonomies • Plan and conduct interviews, user surveys, card sorting and usability tests • Design and execute studies into user behaviour and attitudes • Conduct heuristic evaluations • Help define and refine user personas • Present and communicate insights in order to help shape long-term product strategy • Plan and conduct user research and competitor analysis • Interpret data and qualitative feedback • Create user stories, personas, and storyboards • Determine information architecture and create sitemaps • Create prototypes and wireframes • Conduct usability testing
11	IT Risk Manager (MMGS-II)	• Responsible for identifying IT Risk including Process, Technology, Cyber Security, Audit, Legal and regulatory compliance. Candidate should be a subject matter expert on IT Risk Management with proven leadership capability to manage and drive risk management processes at pan-organization level including business functions • Design enterprise wise IT Risk management framework and supporting implementation. Monitoring of IT Risk in the organization • Primary interface will be within information technology with further engagement with business entity, data, process, and control owners. This role must conduct risk analysis on, but not limited to, information systems, proprietary applications, business processes, surround applications, physical environments, third party service providers, information security tools and tactics, as well as business continuity and disaster recovery capabilities in accordance with established regulations and organization standards • Continuously identify, assess, measure, document and monitor information technology risk by performing independent risk assessments against IT assets, propriety applications, vendor based solutions, business processes and third party relationships • Assist with Risk Management initiatives resulting from risk analysis by developing risk-based corrective action plans along with risk owners and providing oversight in their execution and completion • Operate as a key project and risk-focused resource for technical and architectural reviews, technology projects, new business process, and change management activities • Assist in monitoring and reporting risk management related metrics and status presented to management • Participate in the development of the annual IT Risk Universe and Schedule, maintain the risk register, evaluate new risk threats, and establish control recommendations to mitigate loss of data, confidentiality, integrity and availability • Present identified risk findings to management and negotiate suggested action plans • Stay knowledgeable of current advances in all areas of information technology concerning vulnerabilities, security breaches or malicious attacks • Understanding of latest risk mitigation tools/techniques and their implementation.
12	IT Security Expert (MMGS-III)	• Mitigating IT threats by gathering information and developing plans, Monitoring networks for security breaches, Training users on security protocols, developing best practices and security standards, Creating and testing disaster recovery procedures to keep IT running in the event of a security breach • Responsible for reviewing internally developed applications, before they are deployed in to production environment • Identify the vulnerabilities that can be exploited by potential malicious hacker • The assessment of application consists of tools based testing, and manually testing with a web browser or designated client software • The areas include but not limited to VAPT, Input validation, Access Control, Password Policy, Session Management, Authentication Mechanism, Encryption • Understanding latest IT security tools/techniques • Developing network security standards and guiding network design to meet corporate requirements • Conducting network security assessments and monitoring DDOs, WAF, IDS, firewall, and SIEM systems • Working with internal and external business partners on ensuring that IT infrastructure meet global network security standards • Actively look for security vulnerabilities in our application and network, reporting issues and describing possible solutions. • Design and maintain our security infrastructure. • Stay up to date with security news, keeping an eye out for the latest vulnerabilities and remedies emerging in the field. • Actively liaise with the development team to ensure secure architecture, thorough automated testing of all source code (e.g., via Test-Driven Development). • Provide regular reports auditing our current services and latest changes, as well as our internal practices. • Monitor our server traffic, ticketing and reporting unusual packets. • Developing and designing security devices and software to ensure the safety of internal products and information • Managing security measures for information technology system within a networked system • Operating regular inspections of systems and network processes for security updates • Conducting audit process for initiating security and safety measures and strategies • Customizing access to information per rules and necessity • Maintaining standard information security policy, procedure, and services

13	Project Manager (MMGS-III)	• Build and lead high-performing, agile team focused on Business, Application, Data and Technology Architecture. • Build the Enterprise & Tech Architecture (E&TA) as per internationally established standards and keep the same up to date. • Establish Governance to drive E&TA architecture across the Bank. Ensure the Risks are managed as per the proven practices. • Build enterprise architecture into the change management process. • Review the performance and deliverables of the team and ensure the performance meets stakeholders' expectations. Ensure knowledge upgradation of the stakeholders. • Deliver products/services in alignment with business needs and objectives. Responsible for multiple teams or departments within the Enterprise. • Contribute to IT planning, development of strategies/initiatives and product lifecycle/service orientation; determines current and future needs of IT eco-system. • Oversees portfolio / program / project management responsibilities. Directs financial management and risk management capabilities • Contribute to stable and secure environment, incident management, product health/patching, and the asset management lifecycle. • Assist in the definition of project scope and objectives, involving all relevant stakeholders and ensuring technical feasibility • Develop a detailed project plan to monitor and track progress • Measure project performance using appropriate tools and techniques • Successfully manage the relationship with the client and all stakeholders. Coordinate internal resources and third parties/vendors for the flawless execution of projects. Communicate with vendors, suppliers and executive management to ensure availability of infrastructure, technologies and support. • Perform periodic training on project management and project management related concepts on a periodic basis • Conduct benefits assessments of projects on an on-going basis and reports to appropriate stakeholders • Ensure that all projects are delivered on-time, within scope and within budget • Perform on-going analysis of projects and reports to relevant stakeholders • Create and maintain comprehensive project documentation. • Perform risk management to minimize project risks • Report and escalate to management as needed • Manage changes to the project scope, project schedule, and project costs using appropriate verification techniques • Ensure resource availability and allocation • Should have strong written, verbal and presentation skills
14	Application Architect (MMGS-III)	• Design and validate application architecture design, middleware architecture design and other technology architecture • Estimate design efforts, define detailed schedules, evaluate technologies, develop prototypes, architect design • Change Architecture as per business need and Technology changes • Understand and apply architect principles, processes, their standards and guidelines • Take-up complete ownership of the work assigned in terms of quality and timeliness • Understand, document, and monitor application layering dependencies (User-Interface, Deployment, Public Interface, Application Domain, Application Infrastructure, Technical Frameworks, and Platforms) and application component dependencies. • Understand and monitor impacts to and dependencies between existing technical and network environments. • Define and direct proof-of-concept tasks for proposed architectural interactions. • Monitor software product, supporting tool, and platform licensing taxonomies for compliance and readiness. • Define, plan, propose, and select enabling technologies to support packaged or custom applications. • Prepare approach papers listing technology options, risks, and impacts of various architectural options. • Define data dependencies within, between, and among various applications and application components. • Define and direct coordination among database instances between, and across, various applications and application components. • Document and maintain technical architecture, network architecture, application architecture, and technical application architecture diagrams and descriptions, including releases and versions of software. • Document and maintain context diagrams, functional architectures, data architecture, and messaging architecture diagrams and descriptions. • Ensure that architectural components optimally address business requirements. • Lead / Participate in technical and infrastructure requirements engineering initiatives. • Coordinate with other architects, project managers, and team leads to ensure the development matches the system model. • Coordinate activities with E&TA to ensure broad understanding of architectural approaches and standards across the IT vertical. • Define architecture risk mitigation plans. • Monitor emerging technologies and technical releases from product vendors to evaluate applicability toward current efforts.
15	Technical Lead (MMGS-III)	• Co-ordination with client related to new requirement & support tickets Leading weekly status calls, Tasks allocation & monitoring Team members • Daily status updates to client Code development & bug fixing Code reviews & quality testing HR Functional Set ups (Core HR, Sales service etc.) • Use project's best practices coding standards/secure coding practices. • Prepare and help team to prepare the Design, Coding and Unit testing • Should have a very good understanding of the project architecture • Conduct peer review and provide feedback • Update tracker with accurate information to identify the risk and issues proactively at the sprint level • Conduct project risk identification and mitigation action planning with the PM at the project level • Process check master – to make sure that his team is following all the listed procedures • Constantly looking for ways to increase the team's velocity/productivity by eliminates the waste • People management & Technical management • Assist project manager in the project coordination/management • Report the status with alarms, explanations and solutions • Promptly escalate issues to the reporting manager, Track and resolve issues • Collaborate within a team environment in the development, testing and support of software development project lifecycles • Develop web interfaces and underlying business logic • Prepare any necessary technical documentation • Track and report daily and weekly activities • Participate in code reviews and code remediation • Perform and develop proper unit tests and automation • Research problems discovered by QA or product support and develop solutions to the problems • Perform additional duties as determined by business needs and as directed by management
16	Infrastructure Architect (MMGS-III)	• Designing, articulating and implementing architectural scalability. • Work in close collaboration with application architect to ensure optimal infrastructure design • Draw a long-term enterprise level IT Infrastructure Plan • Ensure that availability requirement are met in the design • Validate all Infrastructure Changes and obtain necessary approvals from competent authority • Interact with IT Partners, Consultants • Evaluate technology, industry trends and identify prospective impact on business • Participate to develop and manage ongoing enterprise architecture governance structure on basis of business & IT strategies • Work as IT consultant and business leaders to develop IT infrastructure solutions • Promote organization architecture process and results to business and IT Departments • Lead and direct to prepare governing principles to guide decision making Equivalent to infrastructure architecture • Draw implementation plan for infrastructure architecture on basis of IT strategies and business requirements • Ensure optimal governance structure and comply with activities related to infrastructure architecture adherence • Enforce infrastructure architecture execution as well as ongoing refinement tasks • Selection and evaluation of infrastructure architecture standards commensurate with IT partners • Consult project teams to fit infrastructure architecture assignments and identify need to modify infrastructure architecture to attain project requirements • Identify need to change technical architecture to incorporate infrastructure needs. • Consult with project teams of infrastructure development to achieve healthy architecture infrastructure • Identify requirements for infrastructures and resources to support infrastructure architecture • Ensure documentation of entire architecture design and evaluation work • Develop & execute education plan for infrastructure architecture
17	Infrastructure Engineer (JMGS-I)	• Installation/ migration/ Up-gradation of WebLogic on Solaris/LINUX/UNIX • Sizing, capacity planning, evaluation and procurement of hardware. • Installation of new equipment, hardware swap-outs and component replacements (servers, network equipment and storage) • Implementation of virtualization. • Installation and maintenance of electrical supplies and equipment. Installation of associated infrastructure such as network patching • Network cabling and testing • Supplier liaison - arranging orders and deliveries with infrastructure vendors • Experience of web application deployment on WebLogic using console & command line • Integration of web servers/application servers and DB servers. • Management of SSL certs on webservers / app servers • Troubleshooting of logs, providing logs on demand from different teams (Architects, developers and validations) • Providing thread /heap dump as per requirement • Working with different teams during production deployment Automation of the tasks using shell scripting • Ensure periodic health checks and take appropriate steps for high availability • Ensure that predefined SLA is maintained • Ensure that 100% BCP is provisioned in all respect • Responsible for implementation of ITIL/ITSM tools (Minimal Manual intervention) • Regular interaction with IT Partners on the Infra roadmap and put up reports to all stake holders • Responsible for Patch Management as per Bank's IT/IS Policy • Regular communication with application owners on above matters • Ensure documentation of entire architecture design and evaluation work • Migration to new systems, capacity planning, performance monitoring and improvement.
18	IT Security Expert (JMGS-I)	• Mitigating IT threats by gathering information and developing plans, Monitoring networks for security breaches, Training users on security protocols, developing best practices and security standards, Creating and testing disaster recovery procedures to keep IT running in the event of a security breach • Responsible for reviewing internally developed applications, before they are deployed in to production environment • Identify the vulnerabilities that can be exploited by potential malicious hacker • The assessment of application consists of tools based testing, and manually testing with a web browser or designated client software • The areas include but not limited to VAPT, Input validation, Access Control, Password Policy, Session Management, Authentication Mechanism, Encryption • Understanding latest IT security tools/techniques • Developing network security standards and guiding network design to meet corporate requirements • Conducting network security assessments and monitoring DDOs, WAF, IDS, firewall, and SIEM systems • Working with internal and external business partners on ensuring that IT infrastructure meet global network security standards • Actively look for security vulnerabilities in our application and network, reporting issues and describing possible solutions. • Design and maintain our security infrastructure. • Stay up to date with security news, keeping an eye out for the latest vulnerabilities and remedies emerging in the field. • Actively liaise with the development team to ensure secure architecture, thorough automated testing of all source code (e.g., via Test-Driven Development). • Provide regular reports auditing our current services and latest changes, as well as our internal practices. • Monitor our server traffic, ticketing and reporting unusual packets. • Developing and designing security devices and software to ensure the safety of internal products and information • Managing security measures for information technology system within a networked system • Operating regular inspections of systems and network processes for security updates • Conducting audit process for initiating security and safety measures and strategies • Customizing access to information per rules and necessity • Maintaining standard information security policy, procedure, and services

19	IT Security Expert (MMGS-II)	• Mitigating IT threats by gathering information and developing plans, Monitoring networks for security breaches, Training users on security protocols, developing best practices and security standards, Creating and testing disaster recovery procedures to keep IT running in the event of a security breach • Responsible for reviewing internally developed applications, before they are deployed in to production environment • Identify the vulnerabilities that can be exploited by potential malicious hacker • The assessment of application consists of tools based testing, and manually testing with a web browser or designated client software • The areas include but not limited to VAPT, Input validation, Access Control, Password Policy, Session Management, Authentication Mechanism, Encryption • Understanding latest IT security tools/techniques • Developing network security standards and guiding network design to meet corporate requirements • Conducting network security assessments and monitoring DDOs, WAF, IDS, firewall, and SIEM systems • Working with internal and external business partners on ensuring that IT infrastructure meet global network security standards • Actively look for security vulnerabilities in our application and network, reporting issues and describing possible solutions. • Design and maintain our security infrastructure. • Stay up to date with security news, keeping an eye out for the latest vulnerabilities and remedies emerging in the field. • Actively liaise with the development team to ensure secure architecture, thorough automated testing of all source code (e.g., via Test-Driven Development). • Provide regular reports auditing our current services and latest changes, as well as our internal practices. • Monitor our server traffic, ticketing and reporting unusual packets. • Developing and designing security devices and software to ensure the safety of internal products and information • Managing security measures for information technology system within a networked system • Operating regular inspections of systems and network processes for security updates • Conducting audit process for initiating security and safety measures and strategies • Customizing access to information per rules and necessity • Maintaining standard information security policy, procedure, and services
20	IT Risk Manager (IS Dept.) (MMGS-II)	• Responsible for identifying IT Risk including Process, Technology, Cyber Security, Audit, Legal and regulatory compliance. Candidate should be a subject matter expert on IT Risk Management with proven leadership capability to manage and drive risk management processes at pan-organization level including business functions • Design enterprise wise IT Risk management framework and supporting implementation. Monitoring of IT Risk in the organization • Primary interface will be within information technology with further engagement with business entity, data, process, and control owners. This role must conduct risk analysis on, but not limited to, information systems, proprietary applications, business processes, surround applications, physical environments, third party service providers, information security tools and tactics, as well as business continuity and disaster recovery capabilities in accordance with established regulations and organization standards • Continuously identify, assess, measure, document and monitor information technology risk by performing independent risk assessments against IT assets, propriety applications, vendor based solutions, business processes and third party relationships • Assist with Risk Management initiatives resulting from risk analysis by developing risk-based corrective action plans along with risk owners and providing oversight in their execution and completion • Operate as a key project and risk-focused resource for technical and architectural reviews, technology projects, new business process, and change management activities • Assist in monitoring and reporting risk management related metrics and status presented to management • Participate in the development of the annual IT Risk Universe and Schedule, maintain the risk register, evaluate new risk threats, and establish control recommendations to mitigate loss of data, confidentiality, integrity and availability • Present identified risk findings to management and negotiate suggested action plans • Stay knowledgeable of current advances in all areas of information technology concerning vulnerabilities, security breaches or malicious attacks • Understanding of latest risk mitigation tools/techniques and their implementation.
21	Infrastructure Architect (MMGS-II)	• Designing, articulating and implementing architectural scalability. • Work in close collaboration with application architect to ensure optimal infrastructure design • Draw a long term enterprise level IT Infrastructure Plan • Ensure that availability requirement are met in the design • Validate all Infrastructure Changes and obtain necessary approvals from competent authority • Interact with IT Partners, Consultants • Evaluate technology, industry trends and identify prospective impact on business • Participate to develop and manage ongoing enterprise architecture governance structure on basis of business & IT strategies • Work as IT consultant and business leaders to develop IT infrastructure solutions • Promote organization architecture process and results to business and IT Departments • Lead and direct to prepare governing principles to guide decision making Equivalent to infrastructure architecture • Draw implementation plan for infrastructure architecture on basis of IT strategies and business requirements • Ensure optimal governance structure and comply with activities related to infrastructure architecture adherence • Enforce infrastructure architecture execution as well as ongoing refinement tasks • Selection and evaluation of infrastructure architecture standards commensurate with IT partners • Consult project teams to fit infrastructure architecture assignments and identify need to modify infrastructure architecture to attain project requirements • Identify need to change technical architecture to incorporate infrastructure needs. • Consult with project teams of infrastructure development to achieve healthy architecture infrastructure • Identify requirements for infrastructures and resources to support infrastructure architecture • Ensure documentation of entire architecture design and evaluation work • Develop & execute education plan for infrastructure architecture
22	Deputy Manager (Cyber Security - Ethical Hacking) (MMGS-II)	• Performing periodic Internal Ethical Hacking and red team exercises comprising Web Application Security Testing , Mobile App security testing, Network, System and Application vulnerability assessment & penetration testing, ICS/IoT device security testing. • Proactively engage with stakeholders, build strong relationships with the management of business and auditors, to facilitate vulnerability discovery and remediation efforts. • Perform security risk assessments that support business requirements, and recommend mitigations and countermeasures to address risks, vulnerabilities and cyber threats • Participate in application security assessments. • Perform network security assessments and security configuration reviews. • Assist in development and implementation of information / cyber security management policies, procedures, and standards based on NIST standards, industry best practices, and compliance requirements.
23	Deputy Manager (Cyber Security - Threat Hunting) (MMGS-II)	• Must have performed Threat hunting on a regular basis • Scripting skills are desirable. • Perform reverse engineering on malware as required to facilitate investigation and analysis • Assessing feeds, events collected and fine-tuning rules as appropriate • Characterize suspicious binaries and be able identify traits, C2, and develop network and host-based IOCs. • Identify potential malicious activity from memory dumps, logs, and packet captures • Interact and assist other investigative teams within organization. • Participate as part of a close team of technical specialists on coordinated responses and subsequent remediation of security incidents.
24	Deputy Manager (Cyber Security - Digital Forensic) (MMGS-II)	• Conduct Forensic examination of digital and other evidences and analyze the incidents for forensic investigations using Forensic Tools (Commercial and Open source tools). • Assist in development and implementation of information / cyber security management policies, procedures, and standards based on NIST standards, industry best practices, and compliance requirements.
25	Security Analyst (MMGS-III)	• Be a senior / L3 level security analyst and shift in-charge of various shifts of SOC operations like Incident Management, VAPT, Infrastructure management etc. • Be the Subject Matter Expert (SME) of SOC areas assigned to you for day to day operations • Perform threat management, threat modelling, identify threat vectors and develop use cases for security monitoring • Lead Threat hunting activities, Incident Management and Forensics analysis. • Ensure all threat intelligence received from 3rd party, regulators and governing bodies are curated and operationalized. • Guide L1 & L2 level officials in the SOC in logs analysis for incident creation, verify correctness of incidents remediation by application / asset owner (AO), guide the AOs for proper remediation, and manage escalation with AOs. • Manage shift takeover and handover activities with proper records for audits • Implement SOPs in the SOC from People, Processes and Technologies standpoint • Ensure SOC technologies are fine tuned to run optimally, securely and reliably. • Responsible for integration of all standard and non-standard logs with SIEM/UEBA/DAM/NBA etc. (as applicable) • Create intuitive dashboards, create rules, signatures, decoders / parsers, models, patterns • Collaborate, coordinate with IT & other stakeholders, build and maintain positive working relationships with them. • Understand cyber-attack tools techniques and procedures, perform in-depth analysis of security logs in an attempt to detect unauthorized behavior and activities. • Prepare management and regulatory reports, MIS • Closely collaborate with stakeholders in IT and others for day to day SOC related operational and tactical standpoint KRA: • Recommend deployment, integration, logs parsing/ decoding techniques, reporting, analysis, remediation, dash-boarding, querying and MIS techniques in the domain of your SOC operations. • Directly responsible to create P1 & P2 incidents as individual contributor • Perform threat management, threat modelling, identify threat vectors and develop use cases for security monitoring. • Individual contributor in Threat hunting activities, Incident Management and Forensics analysis. • Shift in-charge to manage day to day shifts in SOC • Ensure SOC setup itself remains secured fortress • Analysis of critical incidents, mitigation, monitoring, escalations etc. • Enhance capabilities of L1 & L2 personnel resources for in above areas.
26	Manager (Cyber Security - Ethical Hacking) (MMGS-III)	• Managing and leading periodic Internal Ethical Hacking exercise and threat hunting activities. • Proactively engage with stakeholders, build strong relationships with the management of business and auditors, to facilitate vulnerability discovery and remediation efforts. • Perform security risk assessments that support business requirements, and recommend mitigations and countermeasures to address risks, vulnerabilities and cyber threats • Preparation of Standard operating procedures (SOPs) and security solution documents. • Participate in application security assessments. • Perform network security assessments and security configuration reviews. • Performing and leading the Internal Ethical Hacking and red team (IEHRT) exercises. • Ensure timely compliance of Cyber security assessments and Information Systems audits • Assist in development and implementation of information / cyber security management policies, procedures, and standards based on NIST standards, industry best practices, and compliance requirements. • Assist in Developing, implementing and monitoring the cyber security maturity assessment in the Bank. • Assisting in activities related to IS Policy, Cyber Security Policy etc.
27	Manager (Cyber Security - Digital Forensic) (MMGS-III)	• Managing and leading Digital Forensic analysis Activities. • Conduct Forensic examination of digital and other evidences and analyse the incidents for forensic investigations using Forensic Tools (Commercial and Open source tools). • Proactively engage with stakeholders, build strong relationships with the management of business and auditors, to facilitate vulnerability discovery and remediation efforts.

28	Chief Manager (Vulnerability Mgmt. & Penetration Testing) (SMGS-IV)	**Job Profile:** • Lead the VAPT team which conducts Vulnerability Assessment, Penetration, AppSec, Code Review, and Configuration review as also monitors and reports Phishing, Mobile Rogue Apps, Phishing sites. • Set strategic directions and maintain proficiency in sync with Global Best practices and various domestic & global regulatory directions and execute them to enhance VAPT program of the Bank. • Identify vulnerabilities in IT Infra, applications, processes, networking and security setup and provide directions to close the same. • Keep repository of vulnerabilities like plug-ins and signatures upto-date in VAPT tools. • Focus on zero-day vulnerabilities and check for their presence in Bank's environment, collaborate with stakeholders for their remediation and verify the same. • Proactively engage with various internal and external stakeholders like IT, Business, Regulators, Auditors to ensure vulnerabilities remediation are aligned with business and regulatory objectives. • Prepare SOPs for VAPT program including detection and remediation of vulnerabilities. • Lead compliance / remediation verification of vulnerabilities to analyse configurations and facilitate implementation of configurations and hardening settings for networks, operating systems, applications, databases, and other information system component as per statutory, regulatory requirements, guidelines and security best practices. • First point of contact for escalation of all technical and process issues. Provide technical subject matter expertise wherever required by IT departments for timely resolution and mitigation of vulnerabilities. • Provide suggestions to align various policies Information Security Policy, Cyber Security Policy and related procedures as per global and regulatory standards from VAPT standpoint. • Managing the work and workloads of the VAPT team and shift hand-off activities for 24X7X365 SOC operations. • Enhance capabilities of VAPT team through trainings and workshops • Manage shifts of VAPT team for its 24x7x365 days basis operations. **KRA**: • Supervision and management of VAPT program in the Bank and ensuring compliance with various policies like Information Security Policy of the Bank and domestic and foreign regulatory mandates. • Timely detection of vulnerabilities and guiding the stakeholders for their closure. • Adoption of global best practices including tools, techniques, methods, processes and align the Bank's VAPT program accordingly. • Reduce false positive vulnerabilities. • Issue timely advisories to stakeholders on zero-day vulnerabilities. Detect and verify closure of the same. • Automate VAPT processes for detection and closure of vulnerabilities through tools, techniques, methods and processes. • Management reporting through dashboards leveraging analytics. • Design and Implement metrics to manage and measure the VA/PT efforts quantitatively and qualitatively. • Ensure SOC setup itself remains secured fortress • Closely collaborate with stakeholders in IT and others for day to day SOC related strategic, operational and tactical standpoint
29	Chief Manager (Incident Management and Forensics)(SMGS-IV)	**Job Profile:** • Lead the operations of Information and Cyber Security Incident Management (IM) team within SOC as per Bank's Information / Cyber Security Policies, Procedures as also Global standards. • Set strategic directions for the IM team in line with Bank's policies, Cyber Crisis Management Plan (CCMP), regulatory requirements and NIST framework. • 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. • Create playbooks for automating for logs correlation, incident creation, reporting, remediation, escalation & closure verification • Define and optimize Standard Operating Procedures (SOPs), workflows and processes to support the team in consistent, quality execution of security monitoring and detection. • Deeply embed threat intelligence received from various internal and external sources into SOC for Real-time correlation and reporting of potential security incident. • Benchmark SOC Incident Management processes against ISO 27035 standards. • Collaborate with IT and Business units to Respond and Recover from the security incidents. • Ensure continued evolution of threat hunting, monitoring, detection, analysis and Incident respond and response capabilities and processes. • Research on emerging threats and vulnerabilities and development of structured analytical methodologies to utilize threat intelligence inputs. • Manage Red Team / Blue Team exercises at planned intervals on Bank's critical infrastructure to measure Bank's defensive and responsive capabilities towards cyber-attacks. • Provide technical Incident Response guidance to the L1 and L2 Incident handlers for in depth investigations and performing Root Cause Analysis (RCA) to establish complete cyber kill chain • Participate in forensic investigation by analyzing and correlating logs collected by SOC. • Conceptualize, create and demonstrate analytical dashboards and reports to the management. • Ensure timely submission of regulatory returns. • Effectively participate Cyber drills, table top exercises conducted by the Bank and regulators. • Manage the work and workloads of the IM team and shift hand-off activities for 24X7X365 SOC operations. • Enhance capabilities of IM team through trainings and workshops **KRA**: • Manage incident management functions within SOC and ensure process compliance to statutory and regulatory requirements. • Automate Detect, Respond and Recover processes for security incidents • Achieve benchmarking against ISO 27035 • Embed threat intelligence into SOC for real-time proactive threat detection and prevention of potential security incident • Collaborate with IT and Business in finetuning IT setup for implementing playbooks for security orchestration, automation and response • Minimize false positive security incidents • Prioritise incidents into P0, P1, P2, P3 (P0 being cyber-crisis and P3 being Low severity) • Directly responsible to create P0 & P1 incidents as individual contributor • Implement learnings to strengthen SOC monitoring and detection capabilities. • Ensure timely submission of various reports to regulators and internal stakeholders • Participate effectively in forensic investigation leveraging correlated and analysed logs collated by SOC. Arrive at RCA of security incidents • Ensure SOC setup itself remains secured fortress • Closely collaborate with stakeholders in IT and others for day to day SOC related strategic, operational and tactical standpoint
30	Chief Manager (Security Analytics and Automation) (SMGS-IV)	**Job Profile:** • Responsible for SOC Transformation by leading efforts for automating mundane L1/L2 activities such as alert triage, context and enrichment, live threat feeds, incident response etc. • Devising security Monitoring and Analytics automation strategy and Identifying processes that can be automated and orchestrated to ensure maximum SOC efficiency and effectiveness. • Statistical analysis of users and entities to help detect anomalies of users, network, host and content. • Leverage Non-IT contextual data for and various IT systems like PIMS, IAM, DLP and business applications like CBS, HRMS etc. to build strong use cases on user and entity behavior analysis to arrive at potential insider threat by malicious user or compromised systems / user credentials. • Threat intelligence curation and automating it for SOC monitoring tools consumption. • Closely work with IT departments, Threat Intelligence, incident management and Forensics teams to understand, define, develop, and integrate automation and orchestration capabilities. • Managing creation and optimization of security incident playbooks reviewing and validating new Use Cases. • Measurable reduction in mean time to detect (MTTD) and mean time to respond (MTTR) for security incidents. • Issue advisories based on incidents to proactively avoid occurrences of the same in other domains • Issue advisories to stakeholders in IT and Business based on external threat intelligence for taking proactive measures • Enhance SOC capabilities from reactive to predictive SOC • Develop expertise within the SOC and IT teams on security incident management • Maintain knowledge repository of incidents, learning, analysis • Proof of concept (POC) of any new SOC solution/functional modules. • Designing security analytics use cases, Research and Development of emerging threats and technologies, threat intelligence collection, support to other SOC team for product engineering and process improvements. **KRA:** • Automation of L1 & L2 SOC analysts' routine alerts / incidents reporting. • Automating Security Orchestration, Automation and Response activities through playbooks • Measurable reduction in MTTD and MTTR. • Review and validating new Use Cases. • Conceptualize and develop security analytics models leveraging billions of events collated by SOC. • Transform SOC from reactive to predictive SOC • Elevate the capabilities of the SOC to generate absolute material security incidents with severe criticality • Design security analytics use cases, Research and Development of emerging threats and technologies, threat intelligence collection, support to other SOC team for product engineering and process improvements. • Ensure SOC setup itself remains secured fortress • Closely collaborate with stakeholders in IT and others for day to day SOC related strategic, operational and tactical standpoint
31	Chief Manager (SOC Infrastructure Management)(SMGS-IV)	**Job Profile:** • Responsible for managing end to end SOC infrastructure including installation, integration, provisioning, de-provisioning of SOC Infra in UAT and production environment. • Implementation of secured configuration of settings / hardening, closure of vulnerabilities by implementing patches, upgradation of version in SOC Infra setup • Installation of OS, applications, RDBMS, web servers, open source technologies and configure them as per corporate requirements • Integration of It Infrastructure with PIMS, IAM, SSO, AD, AV, ITAM, ITSM, DLP, NAC • Security of IT Infrastructure by deploying security technologies like firewalls, IPS, WAF etc. • Uptime management, manage LAN and integration with corporate network, • Credential / user management, roles and groups management, undertake administrative activities on IT / SOC infrastructure • IT Infra related SLA management with multiple vendors & OEMs • Developing Business Continuity and DR Plan and participate in various DR Drills • Ensure SOC setup reasonably acceptable RTO & RPO. • Ensure SOC setups is in accordance with Bank's policies and regulatory & statutory requirements • Implementation of encryption, hashing techniques for secured communication, processing and storage of data **KRA**: • Managing end to end SOC infrastructure including shipment/placement/replacement and provisioning/ deprovisioning of SOC assets in UAT and production environment. • Manage uptime as per corporate requirement • Keep SOC Infra secured by implementing Secure Configuration Document (SCD) and vulnerability assessment compliance in entire SOC infrastructure. • Maintain Version Upgrades/Patch Management and Control across all the technologies. • Ensure SOC setup itself remains secured fortress • Capacity planning (up gradation of infrastructure-hardware) of SOC. • Backup/Restoration, Tape devices movement, Testing of backup/restoration as per ISMS procedure • Manage acceptable RTO & RPO. • Prove SOC RTO and RPO through various means and during Bank's various DR BCP Drill. • Closely collaborate with stakeholders in IT and others for day to day SOC related strategic, operational and tactical standpoint

32	Chief Manager (SOC Governance) (SMGS-IV)	**Job Profile**: • Lead the Governance team and be responsible for implementing various policies including Information Security Policy, Cyber Security Policy, Data Governance Policy and related procedures • Implement ISO 27001, 27002, 27035 standards • Conceptualize, develop and review various SOPs for SOC operations aligned with policies, standards, procedure and guidelines • Develop strategies, deploy techniques for ensuring security in SOC infrastructure & operations • Track for new versions and patches of various SOC infrastructure and applications released by OEMs and ensure same are deployed by SOC within stipulated time frame • Provide guidance to SOC infra team to close infrastructure and process level vulnerabilities • Ensure core objective of SOC is adhered to including true positive incidents / alerts are sent to stakeholders like IT, Business and individual users as applicable. • Ensure SOC becomes Nerve Centre of every activity which could impact security of the Bank • Review change, patch, user, SoD, uptime managements • Round the clock Health monitoring of SOC infrastructure. • Ensuring SOC devices uptime as per SLA. • Managing DR BCP Drill as per Bank's requirements. • Ensure all statutory and regulatory reporting is done in time bound manner • Ensure all staff members of the Bank and vendor partners are well versed with Information Security related policies, standards, procedures, guidelines and SOPs and are adhering the same in day to day operations • Closely collaborate with stakeholders in IT and others for day to day SOC related strategic, operational and tactical standpoint **KRA:** • Ensure SOC operations are in compliance with various policies. • Achieve and maintain ISO 27001, 27002, 27035 • Implement NIST framework, prescriptions data security laws • Ensure SOC setup itself remains secured fortress • Develop SOPs to ensure SOC operations are managed in secured manner • Timely submission of statutory and regulatory reports
33	Chief Manager (Cyber Security - Ethical Hacking) (SMGS-IV)	• Overall supervision and strategic direction for cyber security program within Bank. • Managing and leading periodic Internal Ethical Hacking exercise activities. • Proactively engage with stakeholders, build strong relationships with the management of business and auditors, to facilitate vulnerability discovery and remediation efforts. • Participate in application security assessments. • Perform network security assessments and security configuration reviews. • Supervising the Internal Ethical Hacking and red team (IEHRT) exercises.
34	Chief Manager (Cyber Security - Digital Forensic) (SMGS-IV)	• Overall supervision and strategic direction for cyber security program within Bank. • Managing, leading and supervising Digital Forensic analysis activities. • Conduct Forensic examination of digital and other evidences and analyse the incidents for forensic investigations using Forensic Tools (Commercial and Open source tools). • Proactively engage with stakeholders, build strong relationships with the management of business and auditors, to facilitate vulnerability discovery and remediation efforts. • Preparation of Standard operating procedures (SOPs) and security solution documents.
35	Chief Manager (Cyber Security - Threat Hunting) (SMGS-IV)	• Overall supervision and strategic direction for cyber security program within Bank. • Managing, leading and supervising Digital Forensic analysis activities. • Conduct Forensic examination of digital and other evidences and analyse the incidents for forensic investigations using Forensic Tools (Commercial and Open source tools). • Proactively engage with stakeholders, build strong relationships with the management of business and auditors, to facilitate vulnerability discovery and remediation efforts. • Preparation of Standard operating procedures (SOPs) and security solution documents.

Remarks: Roles, in addition to the above mentioned Job Profile and KRAs, may be assigned by the Bank from time to time for any Post.

(D) Confirmation Process: The selected candidate's performance will be evaluated through evaluation system and only successful candidates will be confirmed in Bank.

(E) Remuneration:

Sr No	Grade	Scale of Pay
1	Junior Management Grade Scale I (JMGS I)	23700-980/7-30560-1145/2-32850-1310/7-42020
2	Middle Management Grade Scale II (MMGS II)	31705-1145/1-32850-1310/10-45950
3	Middle Management Grade Scale III (MMGS III)	42020-1310/5-48570-1460/2-51490
4	Senior Management Grade Scale IV (SMGS-IV)	50030-1460/4-55870-1650/2-59170

The scale of pay applicable to different grade are furnished above. The official will be eligible for DA, HRA, CCA, PF, Contributory Pension Fund, LFC, Medical Facility etc. as per rules in force from time to time.

(F) 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/ Interview advices etc. by email.

GUIDELINES FOR FILLING ONLINE APPLICATION:

i. Candidates will be required to register themselves online through the link available on SBI website **https://bank.sbi/careers** OR **https://www.sbi.co.in/careers** 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 and intimation charges of Rs125/- (One hundred Twenty Five only) for SC/ST/PWD 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 NOT 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. PWD 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'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 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 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. Selection Process:
(For Post Sr No. 1 to 24):

The selection of candidates for posts Sl No. 1 to 24 will be on the basis of Online Written Test and Interview.

Online written Test: The online written test will be conducted tentatively on 20.10.2019. The call letter of test will be uploaded on Bank's website and also advised to the candidates through SMS and e-mails. Candidates will be required to download the call letters. The test may be held at Guntur, Kurnool, Vijaywada, Vishakhapatnam, Guwahati, Silchar, Bhagalpur, Darbhanga, Muzaffarpur, Patna, Chandigarh/ Mohali, Raipur, Bhilai, Bilaspur, Delhi/ New Delhi, Faridabad, Ghaziabad, Greater Noida, Gurugram, Panaji, Ahmedabad, Vadodara, Ambala, Hissar, Hamirpur, Shimla, Dhanbad, Jamshedpur, Ranchi, Bengaluru, Hubli, Mangalore, Kochi, Thiruvananthapuram, Bhopal, Indore, Aurangabad, Mumbai/ Thane/Navi Mumbai, Nagpur, Pune, Imphal, Shilong, Aizawl, Kohima, Bhubaneshwar, Sambalpur, Puducherry, Jalandhar, Ludhiana, Mohali, Patiala, Jaipur, Udaipur, Bardang/ Gangtok, Chennai, Madurai, Tirunelveli, Hyderabad, Warrangal. Agartala, Allahabad, Kanpur, Lucknow, Merrut, Varanasi, Dehradun, Asansol, Greater Kolkata, Kalyani, Siliguri centres.
CANDIDATE SHOULD CHOOSE THE NAME OF THE CENTRE WHERE HE/SHE DESIRES TO APPEAR IN THE EXAMINATION. NO CHANGE IN THE CHOICE OF EXAMINATION CENTRE WILL BE ENTERTAINED. THE BANK, HOWEVER, RESERVES THE RIGHT TO ADD OR DELETE ANY CENTRE AND ALLOT THE CANDIDATE TO ANY CENTRE OTHER THAN THE ONE HE/SHE HAS OPTED FOR.

Pattern of online written Examination:

Sr No.	Test		No. of Questions	Marks	Time
1	General Aptitude*	Test Of Reasoning	50	50*	90 Min
2		Quantitative Aptitude	35	35*	
3		English Language	35	35*	
4	Professional Knowledge (PK)	General IT Knowledge	25	50	70 Min
		Role based Knowledge	50	100	

* Qualifying in nature and marks thereon will not be reckoned for arriving at the Merit.
(a) Except Professional Knowledge (PK) paper, other papers will be of qualifying in nature. Candidates have to score minimum qualifying marks in these papers. The minimum qualifying marks will be as decided or may be waived at the discretion of Bank. The questions will be bilingual i.e. in Hindi & English. The candidates will have option to answer the questions in Hindi or English (except for test of English Language).
(b) To be eligible for being short-listed for interview, candidates have to score equal to or above the cut-off marks to be decided by the Bank for the PK test, besides scoring equal to or above the Minimum qualifying marks in other tests.

Online written test will be held on-line. If number of applications is less, Bank reserves the right to consider selection of the candidate(s) through short listing and interview, instead of Online written test & interview.

Interview: Adequate number of candidates as decided by the Bank will be called for Interview based on performance in online written test. Interview will carry 25 marks. The qualifying marks in Interview will be as decided by the Bank.

Merit List: The final merit list will be arrived at after aggregating the marks of Professional Knowledge test (out of 150 marks) and interview (out of 25 marks). Weightage of score will be as under:

Grade	Weightage Pattern
JMGS-I , MMGS-II & MMGS-III (Post Sr No. 1 to 24)	• Written Test: 70% • Interview: 30%

The selection will be made from the Top merit ranked candidates in each category.
Note:- In case more than one candidate score the cut-off marks (common marks at cut-off point), such candidate will be ranked according to their age in descending order in select list.

Selection Process:
(For Posts Sl. No. 25 to 35):

The selection of candidates from Post Sl No. 25 to 35 will be based on Short listing and Interview.

Shortlisting: Mere fulfilling minimum qualification and experience will not vest any right in candidate for being called for interview. The Short listing Committee constituted by the Bank will decide the short listing parameters and thereafter, adequate number of candidates, as decided by the Bank will be shortlisted and called 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 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.

I. Call Letter for Online Examination/ Interview:
a. **Online Examination**: The candidates should download their call letter for online examination and an "acquaint yourself" booklet by entering their registration number and password/date of birth, from the Bank's website. **NO HARD COPY OF THE CALL LETTER/ ACQUAINT YOURSELF BOOKLET WILL BE SENT BY POST.**
b. **Interview**: Intimation/call letter for interview, where required, will be sent by email or will be uploaded on Bank's website. **NO HARD COPY WILL BE SENT.**

J. Proof of Identity to be Submitted at the Examination:
The candidates must bring one photo identity proof such as Passport/Aadhar/ PAN Card/Driving License/Voter's Card/ Bank Passbook with duly attested Photograph in original as well as a self-attested Photocopy thereof. The photocopy of Identity proof should be submitted along with call letter to the invigilators in the examination hall, failing which or if identity of candidates is in doubt the candidate will not be permitted to appear for the test.

K. Action Against Candidate Found Guilty of Misconduct:
Candidates are cautioned that they should not furnish any particulars that are false, tampered/fabricated and they should not suppress any material information while filling up the application form.

At the time of examination/interview, if a candidate is (or has been) found guilty of:
(i) using unfair means during the examination or (ii) impersonating or procuring
impersonation by any person or (iii) misbehaving in the examination hall or
(iv) resorting to any irregular or improper means in connection with his/her candidature for selection or (v) obtaining support for his/her candidature by any unfair means, such a candidate may, in addition to rendering himself/ herself liable to criminal prosecution, will also be liable:
a) to be disqualified from the examination for which he/she is a candidate
b) to be debarred, either permanently or for a specified period, from any examination or recruitment conducted by Bank.

The Bank would be analysing the responses of a candidate with other appeared candidates to detect patterns of similarity. On the basis of such an analysis, if it is found that the responses have been shared and scores obtained are not genuine/valid, the Bank reserves the right to cancel his/her candidature.

L. Use of Mobile Phone, Pager, Calculator, or Any Such devices:
(i) Mobile phones, pagers or any other communication devices are not allowed inside the premises where the examination is being conducted. Any infringement of these instructions shall entail cancellation of candidature and disciplinary action including ban from future examinations.
(ii) Candidates are advised in their own interest not to bring any of the banned item including mobile phones/pagers to the venue of the examination, as arrangement for safekeeping cannot be assured.
(iii) Candidates are not permitted to use or have in possession of calculators in examination premises.

M. Biometric Verification:
The Bank, at various stages, may capture thumb impression of the candidates in digital format for biometric verification of genuineness of the candidates. Candidate will ensure that correct thumb impression is captured at various stages and any inconsistency will lead to rejection of the candidate. In case of any candidate found to be not genuine, apart from taking legal actions against him/her, his/her candidature will be cancelled. As such, they are advised not to apply any external matter like mehandi, ink, chemical etc. on their hands.

N: 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, 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 advices 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 category provided, they must fulfill all the eligibility conditions applicable to unreserved category.
viii. Candidates serving in Govt./ Quasi Govt. offices, Public Sector undertakings including Nationalised 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.

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. 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.

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. 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 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 for single post, only the last valid (completed) application will be retained and the application fee/ intimation charge paid for other registration will stand forfeited. Multiple appearance by a candidate for a single post in online written test/ interview will be summarily rejected/candidature cancelled.

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. Outstation candidates called for interview after qualifying in written test/ short listing will be reimbursed the travel fare of AC-III tier (mail/ express only) for the shortest route in India or actual expenses incurred (whichever is lower). 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. BANK RESERVES RIGHT TO CANCEL THE RECRUITMENT PROCESS ENTIRELY AT ANY STAGE.

xviii. The possibility of occurrence of some problem in administration of the examination cannot be ruled out completely, which may impact test delivery and/ or result from being generated. In that event, every effort will be made to rectify such problem, which may include the conduct of another examination if considered necessary.

xix. At the time of interview, the candidate will be required to provide details regarding criminal cases(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.

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/careers** OR **https://sbi.co.in/careers**)

The Bank is not responsible for printing errors, if any

Mumbai
Date: 06.09.2019

GENERAL MANAGER
(CRPD)