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

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

1. Assistant Manager (Security Analyst) JMGS-I

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

Job Profile and KRAs :

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

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

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

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

Job Profile and KRAs :

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

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

3. Manager (Security Analyst) MMGS-III

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

Job Profile and KRAs :

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

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

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

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

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

Job Profile and KRAs :

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

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