Position	Manager - IT Network and Security
Job Description / Responsibilities	**Network Management:** 1. Oversee and manage the company's network architecture, including LAN, WAN, wireless networks, and VPN. 2. Design, implement, and maintain network infrastructure to ensure efficient and reliable connectivity. 3. Monitor network performance, troubleshoot issues, and implement solutions to improve performance. 4. Coordinate network upgrades and expansions to meet organizational growth and technology needs. 5. Manage and maintain routers, switches, firewalls, load balancers, and other network devices. 6. Ensure high network availability and business continuity through redundancy, backup systems, and proactive monitoring. **Security Management:** 1. Develop, implement, and enforce network security policies and procedures to safeguard the organization's data and assets. 2. Configure, monitor, and maintain firewalls, intrusion detection/prevention systems (IDS/IPS), VPNs, and anti-malware software. 3. Manage and optimize the use of security information and event management (SIEM) tools, intrusion detection/prevention systems (IDS/IPS), endpoint detection and response (EDR), and other security technologies within the SOC. 4. Manage the SOC team in identifying, analyzing, and responding to security incidents and alerts in real-time, ensuring that appropriate response protocols are followed. 5. Incident Lifecycle Management: Oversee the full lifecycle of security incidents, from detection and analysis to containment, remediation, and recovery, ensuring all steps are well-documented. 6. Root Cause Analysis: Facilitate the identification and analysis of the root cause of security incidents, ensuring that findings are documented and lessons learned are communicated to prevent future occurrences. 7. Conduct regular vulnerability assessments and security audits to identify and mitigate potential risks. 8. Ensure SEBI and RBI related compliance with security standards, frameworks, and industry regulations. 9. Respond to and manage network security incidents, including identifying, analyzing, and remediating security breaches. 10. Manage user access controls and authentication systems to ensure proper security measures are in place. 11. Manage integration of WAF solutions to protect web applications and APIs across the organization. Configure, monitor and manage WAF policies, custom rules, and security settings to ensure comprehensive protection from common attack vectors. **Office 365 Administration:** 1. Manage and administer all aspects of the Office 365 platform, including Exchange Online, SharePoint Online, Microsoft Teams, OneDrive for Business, and other O365 services. 2. Create, modify, and manage user accounts, groups, mailboxes, and licenses in the Microsoft 365 Admin Center. 3. Configure and maintain security settings and policies for Exchange, SharePoint, and Teams to ensure data protection and compliance. 4. Manage Office 365 tenant settings, including user authentication, federation, and single sign-on (SSO) configurations. 5. Perform regular maintenance and updates to the O365 environment to ensure optimal performance, including managing updates, patches, and features. 6. Provide configuration and troubleshooting support for O365 applications and services. 7. Implement and maintain security policies for O365 services, such as multi-factor authentication (MFA), conditional access, data loss prevention (DLP), and encryption.

	8. Manage and monitor Office 365 security and compliance settings, including auditing, data retention policies, eDiscovery, and compliance reporting. 9. Stay up-to-date with Microsoft's O365 security and compliance features and provide recommendations for continuous improvement. 10. Collaborate with security teams to resolve issues related to data protection and compliance. 11. ATP Configuration and Management: Configure and manage Advanced Threat Protection (ATP), including Safe Links, Safe Attachments, Anti-Phishing policies, and Anti-Spam settings to protect against email-based threats. **Monitoring & Reporting:** 1. Develop, Implement and maintain monitoring tools to ensure network performance and security are consistently maintained. 2. Provide regular reports to senior management on network and security performance, incidents, and risk mitigation activities. 3. Maintain and update documentation related to network infrastructure, security procedures, and disaster recovery plans. 4. Disaster Recovery & Business Continuity: 5. Develop and maintain disaster recovery plans to ensure minimal downtime in case of network outages or security breaches. 6. Implement business continuity protocols and processes to minimize the impact of disruptions on the organization. **Skills & Competencies:** ➢ Strong troubleshooting, analytical, and problem-solving skills. ➢ Excellent knowledge of network protocols (e.g., TCP/IP, DNS, HTTP, SNMP). ➢ Familiarity with security technologies such as firewalls, IDS/IPS, VPNs, endpoint protection, and encryption. ➢ Experience with network monitoring tools and security information and event management (SIEM) solutions. ➢ Strong communication skills, both verbal and written, with the ability to communicate technical information to non-technical stakeholders. ➢ Ability to work under pressure and manage multiple priorities in a fast-paced environment. ➢ Understanding of cloud networking and security, including hybrid cloud environments. **KEY RESPONSIBILITIES AND ACCOUNTABILITIES** ➢ Responsible for Network and O365 uptime and Security Compliance ➢ To manage Network infrastructure and Security compliance within the framework of Regulatory guidelines. ➢ Coordination with Bank IT team for Network and Security related requirements for the hosted environment in Bank Data centers. ➢ Any other work may be assigned from time to time. ➢ Provide regular updates to the immediate superior as and when required. ➢ **Vendor Coordination:** Coordinate with third-party service providers (telecom operators, MPLS providers) for provisioning, troubleshooting, and maintaining leased line and MPLS services. ➢ **Vendor SLA Compliance:** Ensure that service providers meet their contractual obligations regarding uptime, bandwidth, and performance metrics, and address any service disruptions or deficiencies. ➢ Security Awareness Training: Promote ongoing security awareness for the organization as a whole, including conducting training sessions on best practices and threat awareness.
Job specific skills	Applicants should have – ➢ Prior experience in a similar role will be preferred. ➢ Excellent oral & written communication skills. ➢ should have sound understanding of capital markets. ➢ Should be result-oriented, self-starter, proactive. ➢ Ability to work independently and also as part of a team

Educational Qualification	Graduate/ post-graduate from recognized Universities, Advanced degree preferred.
Minimum Experience	8+ Years
CTC OFFERED	Compensation will not be a limiting factor for the right candidate and will be discussed on a case by case basis.
Location of posting	Mumbai
How to apply	Applications should be submitted on our email careers@bobcaps.in Please mention **"Application for the post of Manager IT Network and Security"** in the subject. Applications with any other subject will not be accepted.
Website	www.bobcaps.in