7. Scope of Work

Central Bank of India intends to procure Cyber Security Solutions and associated Hardware including Storage to meet Banks future business requirements and to appoint a proven & experienced Bidder to Supply, Install/Implement, Configure and Integrate new Cyber Security Solutions into the existing SIEM and SOAR Solution.

- Data Centre (DC) of the Bank is in Navi Mumbai. Disaster Recovery Centre (DRC) is located at Hyderabad.
- The Bank has envisaged the procurement of New Cyber Security Solutions and associated hardware, details of the same have been provided in Annexure 1: Bill of Materials. The Bidder is required to quote the Cyber Security Solutions in compliance to the Technical Specifications given in Annexure 2: Technical Specifications.
- Procurement of the Cyber Security Solutions and associated hardware mentioned in the RFP will be at Bank's discretion and Bank may not procure all the items mentioned in the RFP. Also, Bank may ask for staggered delivery of some of the Cyber Security Solutions and associated hardware mentioned in the RFP. Details of the same would be shared with the successful Bidder at a later stage.
- Bidder must provide the details of each individual proposed Cyber Security Solutions and associated hardware along with the Hardware & Software proposed, in Annexure 1: Bill of Materials.
- Whatever is required for the successful implementation of the proposed cybersecurity solutions, such as x86 based Hardware including any OS, VMs and Load Balancer etc., the Bidders has to provide the same.
- Also, bidder is required to provide the necessary co-hosting details for the proposed solutions in terms of space, power and cooling requirement. However, the same shall be provided by the Bank.
- Bidder is also required to provide the number of ethernet ports (with speed) required for all the Proposed Solutions. However, the same shall be provided by the Bank.
- All the services/solutions offered should be modular, scalable, and should be able to meet Bank's requirements during the period of contract.
- All the services/solutions in scope needs to be designed and implemented with adequate redundancy and fault tolerance to ensure compliance with Service Levels for uptime as outlined in this RFP.
- It should be ensured that during installation/implementation and during operations of the security solutions; none of the existing infrastructure/ business of the Bank should be impacted.
- Bidder is also required to carry out activities given in the following table

Sr. No.	Activity	Remarks
1.	Physical delivery of Cyber Security Solutions and associated hardware	Bidder must supply and deliver the Security Solutions and associated hardware mentioned in Annexure 1: Bill of Materials at the Bank's site and in compliance to the Annexure 2 - Technical Specifications given in the RFP
2.	Installation, configuration & implementation of Cyber Security Solutions and	OEM / OEM Authorised Partner is required to install, configure and implement the Cyber Security Solutions and associated hardware provided by the OEM/s. Thus, OEM /

	associated hardware to suit the requirements.	OEM Authorised Partner is required to unpack, assemble, mount, and boot the solutions/equipment and install the necessary service packs, patches, and fixes to the Operating System, set up and configure the solution. Compatibility issues of subsystems with OS, respective drivers, firmware, any other cards to be installed, if required, are to be resolved by Bidder. OEM / OEM Authorised Partner is required to ensure the successful implementation of the Cybersecurity Solutions part of this RFP.
		Bidder should supply, install, configure, integrate the Cyber Security Solutions and associated hardware. Bank's existing System Integrator and the Bank will conduct the acceptance test and verify that the installation complies with the configuration and relevant setting provided by the Bank's existing System Integrator. In case of new solution proposed for the existing solution, in such case bidder is required to do migration of data to the new proposed solution. The sole responsibility of migration lies with the bidder.
3.	Provide warranty and AMC/ATS support for the tenure of the contract	Bidder will be responsible to provide the following services during the Contract period • Onsite comprehensive warranty from OEM, • AMC/ATS from the OEM • Arrange back-to-back support from the respective OEMs. Bidder is required to submit proof (Certificate / mail from oem / letter etc) of back-to-back support from OEMs. In Case of RMA, it is bidder responsibility to replace the equipment as per SLA and to return the faulty equipment to the OEM warehouse at no extra cost to the Bank during the tenure of the contract.
4.	Complete Migration of Data and Policies from existing solutions to new solutions (if applicable)	Bidder will be responsible to ensure complete migration of data and policy from existing solutions of IT Governance, Risk and Compliance (GRC), Decoy (Honeypot), NAC and Mobile Device Management (MDM) to the newly proposed solutions. Complete Migration from existing to new solutions The sole responsibility of migration lies with the bidder.

- Considering the nature of the Security Solutions, it may happen that the bidder may propose a solution suite consisting of multiple features, functionalities suiting to the RFP requirements and in compliance of RBI cyber security circulars. The bidder shall provide the solutions with all such features (over and above to technical specifications) without any additional cost to the Bank. All the available functionalities should be available to the Bank. The bidders shall include all necessary expenses in complete cost of the respective line items of the solution in Annexure – 1: Bill of Material. All costs shall be included in the line items only.

- The solutions should include all components and subcomponents like software licenses, accessories, and the bidder should supply any other components that is required for the successful installation and commissioning of the solutions that are part of this RFP (if not specified in the Bill of Materials) at no additional cost to the Bank. The bidder should consider all the components required for the successful installation and commissioning of the solutions that are part of this RFP while quoting price for the solutions.
- It is the bidder's responsibility to ensure complete migration of data and policy from the existing solutions of IT Governance, Risk and Compliance (GRC), Decoy (Honeypot) and Mobile Device Management (MDM) to the newly proposed solutions as per Bank's requirement.
- Bidder to ensure that the complete installation and commissioning of all the solutions part of this RFP to be done by the respective OEMs or by OEM Authorised Partners till the successful implementation of the respective solutions. OEMs to provide the certification of authorization for their respective partners.
- After the successful implementation of the solutions by the OEM's, Bidder and OEM to ensure complete handover process is performed from the OEMs to the Bidder team including all documentation.
- The Bidder must Supply, Install/Implement, Configure and Integrate the Cyber Security Solutions and associated hardware into the existing SIEM, PIM, any other such security Solution. Bidder must also provide subsequent comprehensive on-site warranty/AMC/ATS for the proposed Cyber Security Solutions (Hardware, Software, etc.) and associated hardware as per the Bill of Materials shared by the Bank. The delivery plan must be synchronized with the project delivery timelines of the Bank.
- Bidder is also required to provide skilled resources that may be required for the successful completion of the project.
- The Cybersecurity Solutions Hardware should be provided with 3 years of on-site comprehensive warranty which will start from the date of acceptance of Cyber Security solution. Subsequently, Bidder shall provide the AMC support for the remaining two Years post warranty period.
    - The warranty will start only after acceptance of Installation.
    - The Bidder has to submit proof for back-to-back agreement with the Hardware and Software OEM.
- The Cybersecurity Solutions Software should be provided with 1 years of on-site comprehensive warranty which will start from the date of acceptance of Cyber Security solution. Subsequently, Bidder shall provide the ATS support for the remaining four Years post warranty period.
- Bidder is required to co-ordinate with Bank's existing System Integrator for monitoring and troubleshooting for support, throughout the tenure of the contract.
- Bank has option to extend contract period for additional 2 years at the same prices quoted for AMC/ATS of 5th year for in scope components of this RFP.
- The bidder should have a 24x7X365 days support contact center in India in order to log the calls. The contact center numbers should be provided to the Bank along with the escalation matrix mentioning the contact person's name, number and designation in the company
- The bidder should provide 24*7 support for any kind of issue in functionality/performance/integration of the platform during the entire tenure of contract. In

case, the issue is not resolved for more than 8 hours, support personnel has to escalate as per the escalation matrix. The bidder shall provide the details of support team and escalation matrix for immediate assistance to bank's team for any issue.

- No external remote access will be provided for any issues. Bidders are required to provide onsite resources.
- OEM should be present in India for more than 3 years and preferably should be having support centre in India.
- The solution deployed should be compliant with Bank's IS, IT and Cyber Security policies, internal guidelines, regulatory requirements and countrywide regulations and laws.
- The Bidder would be responsible for supply, installation, testing, commissioning, configuring, Operation & Maintenance of the solutions, warranty and AMC of licenses (hardware, software, middleware supplied) as part of this RFP for a period of Five (5) years.
- The contract will be for a period of FIVE years from the date of Go-live.
- During the tenure of the contract, all upgrades or requirements in hardware, software, licensing, implementation of upgrades/patches/version changes etc., due to whatsoever reason including but not limited to EOL or EQS, would be done by the bidder without any additional cost to the bank.
- If a solution fails to meet the technical requirements of RFP during the implementation/before sign-off phase, Bank reserves the right to reject the solution with no cost to the Bank and recover all payments made for that solution. However, in such cases the bidder may offer alternate solution to the Bank which fulfils technical requirements of the RFP with no extra cost to the Bank.
- If during the contract period, the solution is not performing as per specifications in this RFP, bidder shall upgrade/enhance the devices or place additional devices and reconfigure the system without any extra cost to the bank till the required performance is achieved.
- All the Cyber Security Solution must be tightly integrated with SIEM, SOAR, UEBA,PIM,IT Service Desk (Call Logging System), any other such solution.
- The Bidder is required to Integrate all Cyber Security solutions and associated hardware with SOAR, SIEM, PIM and existing ticketing Solution
- All Solutions must be implemented by OEM / OEM authorized service Partner only. In case of OEM authorized partner, valid document should be provided by the OEM for authorising the partner.
- Training – overall for 10 participants for minimum 1 week on all the solutions part of this RFP; Training from OEM / OEM authorized service Partner. Bidder has to provide the same at no additional cost to the Bank.
- **OEM's Assessments Reports**
  Bidders must ensure that all the above solutions are being assessed by the respective OEM's of the proposed products

  i. Respective OEMs to check that the proposed functionality that are part of RFP including technical specifications are working properly
  ii. Assessment is to be performed twice in a year post successful installation for year one and performed once in year for remaining years, during the period of contract.
  iii. OEM to submit and present the reports to bank. In case of any findings, bidder is required to bridge those gaps as per the recommendations of the OEMs during the tenure of contract, at no additional cost to the bank.

7.1 Detailed Scope of Work

The Bidder is required to supply, install, integrate, maintain, and provide AMC for the following (Cyber Security Solutions and associated hardware mentioned in subsection) solutions for the period of contract at Bank's offices. In case of any compatibility issue arises between the proposed solutions/appliance and existing SIEM setup during implementation or within 3 months of installation signoff, then the successful bidder is required to replace such solutions/appliances, with the compatible one, at no additional cost to the bank within 4 weeks of the issue being intimated by Bank.

- The proposed solution should be tightly integrated with all the existing tools / setup and new infrastructure /Assets of the Bank. The selected bidder should implement and maintain these Cyber Security Solutions and associated hardware for Bank's Infrastructure for a period of contract.
- The selected bidder should provide detailed solution document, project implementation/migration plan, new architecture diagram (HLD and LLD) and provision for hosting the proposed solution.
- For the solutions in scope, the Bidder is required to propose appliance, Hardware or software or a combination of hardware and software to meet the individual requirements put forward by the Bank for the respective solutions. Bidder is required to Design, size, supply, install & maintain the required security solutions for the period of contract.
- Bidder is required to Supply, Install/Implement, Configure and Maintain the following Cyber Security Solutions and associated hardware for the period of contract -
    1. Data Discovery & Classification
    2. File Upload Security
    3. Attack Surface Management (ASM)
    4. Breach and Attack Simulation (BAS) along with Red Team Solution
    5. Phishing Simulation
    6. AD Security
    7. IT Governance, Risk & Compliance
    8. Decoy (Honeypot)
    9. Mobile Device Management
    10. Secure Data Backup and Recovery (Ransomware Protection)
    11. Network Access Control (NAC)

- In case of refresh items, that are part of the bill of material, wherein the bidder is proposing new solutions for the existing solutions implemented at Bank, the bidder is required to perform complete migration of all the data from the existing solution to the new solution.
- Bidder is required to refer to tab "Solutions Sizing" in Annexure 2 – Minimum Technical Specifications for guidelines for sizing and licensing of the above solutions.

7.1.1 Data Discovery & Classification

- The bidder is required to Supply, install and Maintain Data Discovery & Classification solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material s given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.

- The proposed data discovery and classification solution should be tightly integrated with the existing DLP Solution.
- Solution should improve Data Loss Prevention Accuracy and should offer seamless integration with existing DLP Solution. DLP solution should leverage the use of this tool.
- Solution should provide visibility of critical data in the Bank.
- Solution should raise security awareness among end users and educate them on data handling.
- Proposed Solution should enable to establish a policy-driven foundation that helps to identify and classify sensitive data at creation, in motion, or at rest and apply the right security policy to protect it. Solution should work with email and office applications as a part of user's day-to-day workflow for identification and classification of mails and documents.
- Policy engine of proposed solution should provide granular options to build policies based on various conditions like AD user, department, file content, file attributes, recipients, location, printer, etc., and these policies shall be triggered based on different Events like creating a new file, opening an existing file or emailing a document, etc.
- Solution should classify other file/file types on Windows OS and the functionality is part of the same endpoint agent. For all other files, Solution must classify the file based on file attributes (file location, file size, file name or based on logged in user etc.)
- Solution should provide a breadth of tools that enable customers to detect sensitive data with Regex, Smart Regex, Categorization using Machine Learning (ML) and natural language processing capabilities do detect PCI, PII, etc., The solution should also be configured to detect specific keywords that may be critical for the Bank.
- Solution must capture time sensitivity of a document. Example - Financial statement needs to be classified confidential until public release on 1st April and post that it should be classified as public.
- The Bidder shall involve their resources in Data Collection, Policy/Rule Creation/Fine-Tuning, Policy/Rule Enforcement and Incident Management Support.
- The tool shall be capable to perform the data classification as per Bank's data classification policy
- Bidder shall conduct awareness programs among end users as and when Bank requires.
- Sizing Guidelines for all the solutions can be found in Annexure 2 - Minimum Technical Specifications, in the sub titles "Solutions Sizing".
- Data Discovery and Classification solution should provide actionable reports, such as but not limited to below mentioned reports:
    1) Data Inventory Reports **-** The Data Discovery and Classification solution should provide comprehensive list of data assets across the Bank, show where sensitive data resides, identify data formats (structured, unstructured, semi-structured) and provide information on data size and growth.
    2) Data Classification Reports - The Data Discovery and Classification solution should classify data based on sensitivity levels, identify data owners and custodians, show who has access to sensitive data and analyse how data is being used.

7.1.2 File Upload Security

- The bidder is required to Supply, Install and Maintain "File Upload Security" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure File Upload Security at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, File Upload Security at DRC should act as Primary
- The proposed File Upload Security solution should proactively prevent cyber threats from entering a network through files. It should act as a pre-emptive shield against malicious content hidden within documents, emails, or other downloadable files.
- The proposed File Upload Security solution should Disarm Malicious Content and Preserving Functionality.
- The proposed File Upload Security solution should Enhanced Protection, Zero-Day Threat Protection and Improved User Experience.
- The file upload / download sources are
    1. Email (/attachment)
    2. WAF
    3. SFTP and
    4. API
    5. Other channels in Bank
- Sizing Guidelines for File Upload Security can be found in Annexure 2 - Minimum Technical Specifications, in the sub tab titles "Solutions Sizing".
- File Upload Security solution should provide actionable reports, such as but not limited to below mentioned reports:
    1. Threat Detection Reports – The File Upload Security solution should provide information on identification of files containing malware, viruses, or other threats, identification of files containing exploits or vulnerabilities.
    2. File Analysis Reports - The File Upload Security solution should provide identification of file types and formats scanned, detection of abnormally large or small files, identification of sensitive data within files, information of embedded objects/scripts and verification of file format integrity.
    3. Incident response reports - The File Upload Security solution should be able provide detailed information about specific file , it's object ,properties and behavior if found malicious or suspicious.

7.1.3 Attack Surface Management (ASM)

- The bidder is required to Supply, Install and Maintain "Attack Surface Management" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure ASM solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, ASM Solution at DRC should act as Primary
- The proposed Attack Surface Management (ASM) solution should reduce the risk of cyberattacks by providing a comprehensive view of your organization's attack surface and proactively addressing vulnerabilities.
- The proposed ASM should provide visibility of attack surfaces as all the potential entry points for a hacker. This should include devices, applications, data, systems, and even your online

presence. ASM should continuously discover and inventory all IT Bank's assets, both internal and external to your network.

- The proposed ASM should provide vulnerability assessment in terms of identifying weaknesses within those assets. This might involve outdated software, misconfigured systems, or weak passwords. By pinpointing vulnerabilities, Bank's / SI's IT team should prioritize patching and remediation efforts.
- The proposed ASM solution should reduce attack points; by removing unused systems, hardening configurations, or segmenting your network to limit access to critical resources.
- The proposed ASM should support proactive threat detection by analysing how attackers might exploit those weaknesses. By simulating attacker behavior (ethical hacking), ASM should identify potential attack vectors and take steps to mitigate them before they're used in a real attack.
- The ASM Solution should be tightly integrated with the Bank's existing solutions, but not limited to, such as Antivirus, EDR, HIPS, VA Scanner, Active Directory, NIPS, NGFW, Sandboxing, Anti APT or any other solution that bank currently has or will procure in the future.
- The proposed ASM solution should tightly integrate with existing security tools (SIEM, SOAR) tools.
- Sizing Guidelines for Attack Surface Management can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- Attack Surface Management solution should provide actionable reports, such as but not limited to below mentioned reports:
  1. Asset Inventory Reports – The Attack Surface Management solution should identify all assets exposed to the internet, categorize assets based on criticality and sensitivity, assign responsibility for asset management and detect unauthorized IT resources.
  2. Vulnerability Assessment Reports - The Attack Surface Management solution should identify vulnerabilities in assets, rank vulnerabilities based on risk, tracks patch management status and evaluate the likelihood of successful exploitation.
  3. Risk Assessment Reports – The Attack Surface Management solution should quantify the potential impact of vulnerabilities, correlate vulnerabilities with known threats and assess the potential impact on business operations
  4. Exposure Reports - The Attack Surface Management solution should list exposed services and their vulnerabilities, identify all domains and subdomains, evaluate the risk posed by vendors and partners
  5. Remediation Reports - The Attack Surface Management solution should track progress in addressing vulnerabilities and support incident response strategies.
  6. Compliance Reports - The Attack Surface Management solution should provide documentation for security audits.

7.1.4 Breach and Attack Simulation (BAS) with Red team solution

- The bidder is required to Supply, Install and Maintain "Breach and Attack Simulation (BAS) with Red team solution" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Breach and Attack Simulation (BAS) with Red team solution solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Breach and Attack Simulation (BAS) with Red team solution at DRC should act as Primary

- The Bidder should Supply, Installation, commissioning, integration, maintenance, and operations of the BAS solution as per the required technical specifications, in both DC & DR
- The Bidder should assist the Bank in identification of the zones to deploy BAS agents along with required prerequisites for connectivity between the attacker machine and BAS agents, and between attacker machines and Threat library
- The Bidder should activate all Attack Modules across all Threat Vectors - Network, URL Filtering, Endpoint, WAF, Email and Data Exfiltration - to simulate real-world attacks and proactively test the Bank's defences in a risk-free environment using pure 'simulation' approach, without causing any harm to the Bank's production environment
- The Bidder should integrate all relevant technology solution components and integrate the BAS platform with the existing SOC Platform of the Bank. Configuration and fine tuning of the platform on continuous basis
- The Bidder should assist the Bank to create and execute various threat campaigns on Endpoints, Servers, Email, Perimeter devices like Firewall, IDS, IPS, etc. as prescribed by the Bank. This should include campaigns for Ransomware, Emerging Threats, Attacks targeted towards Banking & Financial Institutions, Campaigns from BFSI-focused APT Groups, etc.
- The Bidder should provide guidelines to determine the critical threat campaigns / attacks that should be simulated in the Bank's environment. Update the Bank about new threat campaigns / attacks that are added to their threat library on a regular basis
- The Bidder should provide vendor-specific mitigation recommendations for all supported technologies deployed in the Bank. Assist the bank's security operations team in implementation of vendor-specific mitigation recommendations (signatures) for prevention controls (like NGFW, IPS, WAF) TO improve the Bank's security posture on a regular basis.
- The Bidder should integration of the BAS platform with the SIEM, SOAR, EDR, XDR Solution for detection visibility, understanding detection capabilities post execution of threat campaigns, assist in implementation of mitigation recommendations (missing logs and alerts) for detection controls
- The Bidder should use the 'Assumed Breach Approach' to perform Automated Red Teaming on the Bank's systems with pre-specified goals to identify the real attack paths (not all hypothetically possible)
- The Bidder should continuously discover attack paths that lead to the Bank's critical assets, enabling full visibility into the Bank's security posture
- The Bidder should discover hidden elements throughout the Bank's network that enable environment enumeration, lateral movement and privilege escalation
- The Bidder should conduct two health-checks every year to check BAS platform as per best practices and/or recommended configuration and provide the health check document. Conduct the implementation of upgrades/ patches/ version changes during the tenure of the contract
- The Bidder should assist the Bank in the preparation of monthly/quarterly reports which include threat campaigns executed, security posture rating, prevention and detection scores, MITRE ATT&CK mapping, security posture improvement
- The Bidder should enable the Bank's security team members with Red Teaming and Blue Teaming oriented cybersecurity trainings without any additional charge
- Breach and Attack Simulation solution should provide actionable reports, such as but not limited to below mentioned reports:

1. Threat Simulation Reports - The BAS solution should simulate attacks based on real-world threat actor tactics, techniques, and procedures (TTPs), should evaluate the ability of Bank's security tools to detect simulated attacks, and assess the effectiveness of Bank's incident response plan.
2. Security Control Effectiveness Reports - The BAS solution should evaluate the effectiveness of security controls in preventing or detecting attacks, should highlight areas where security controls are lacking, and should suggest improvements to enhance control efficiency.
3. Attack Path Analysis Reports - The BAS solution should be able to visualize how an attacker could move laterally within the network, identify sensitive data exposed to potential attackers and recommend steps to block attack paths.
4. Executive Summaries - The BAS Solution should provide high-level overview which summarizes key findings and recommendations.

- A red teaming solution should provide a comprehensive assessment report of the Bank's security posture by simulating real-world attacks, which should help Bank's team in understanding the Banks's vulnerability landscape and prioritizing remediation efforts.

7.1.5 Phishing Simulation

- The bidder is required to Supply, Install, configure and maintain "Phishing Simulation" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Phishing Simulation solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Phishing Simulation Solution at DRC should act as Primary
- The proposed Phishing simulations should test your Bank's employees' ability to identify and respond to phishing attacks. These simulations mimic real-world phishing emails, text messages, or even phone calls in a controlled environment.
- The proposed phishing simulation solution should support features such as Raising Security Awareness, Identifying Susceptible Employees, Improving Overall Security Posture, and Testing Security Controls.
- By conducting phishing simulations regularly, it should significantly improve Bank's ability to defend against phishing attacks, a common and evolving cyber threat.
- The platform shall facilitate creation of phishing campaigns including QR code phishing which can be customized by bank.
- The bidder should provide services for conducting simulated phishing, vishing and smishing exercises to improve cyber security awareness of bank staff, vendor employees, employees in Overseas branches, employees in Bank's subsidiaries and Board of Directors etc. The resource for conducting the simulated phishing, vishing and smishing exercises shall be deployed in Hyderabad/Mumbai and shall be responsible to complete the exercises as per bank's requirement and submit the report.
- The bidder should provide daily, weekly, monthly status reports or as and when needed by the Bank.
- The bidder should be responsible for delivering social engineering exercises related to simulated vishing and smishing for the tenure of contract.
- The bidder should be capable of performing vishing exercises in both automated and manual methods. The automated approach shall support scalability in conducting vishing campaigns

through Bidder's infrastructure/gateway.

- Sizing Guidelines for Phishing Simulation can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- The Phishing Simulation solution should provide actionable reports, such as but not limited to below mentioned reports:
  1. Campaign Performance Reports – The Phishing Simulation solution should report on the percentage of users who clicked on phishing links, percentage of users who opened phishing emails, should identify Bank's departments with higher susceptibility, average time taken by users to report a phishing email and measure the success of the phishing simulation.
  2. User Behavior Reports - The Phishing Simulation solution should report individual user performance and identify users who consistently fall for phishing attempts.
  3. Training Effectiveness Reports - The Phishing Simulation solution should measure the effectiveness of security awareness training, should tracks changes in user behavior after training.
- Threat Intelligence Reports - The Phishing Simulation solutions should update threat vectors/Library with emerging phishing tactics and techniques and help in Identification of potential threat actors targeting the Bank.

7.1.6 AD Security

- The bidder is required to Supply, Install, configure and maintain "AD Security" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure AD Security solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, AD Security Solution at DRC should act as Primary
- AD Security solution should enhance Active Directory (AD) defences by enforcing access controls, monitoring privileged accounts, and detecting anomalous activities. The proposed solution should protect against insider threats and external attacks, ensuring the integrity and confidentiality of AD infrastructure critical to Bank's operations and data security.
- The bidder is required to Supply, Install, configure and maintain "AD Security" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- The proposed AD Security solution should protect the critical Active Directory (AD) services that manage identities and access throughout a network, that is name a few, control System Access, should protect Credentials and also should reduce the attack surface.
- The Proposed AD Security Solution should support breadth of capabilities to audit, monitor, harden, and secure AD.
- There are several steps Bank can take to improve their AD security. The bank should follow best practices such as "use Strong Passwords", "Enforce complex passwords, Least Privilege, Regular Monitoring and finally software and finally Keep Software Updated.
- The proposed AD Security Solution should support following features such as:
  1. Audit Accounts & Privileges
  2. Attack Path Discovery

3. Real-Time Protection and
4. AD Backup & Recovery

- Sizing Guidelines for AD Security can be found in Annexure 2 - Minimum Technical Specifications, in the sub tab titles "Solutions Sizing".
- The AD Security solution should provide actionable reports, such as but not limited to below mentioned reports:
  1. User-Related Reports – The AD Security Solution should identify users who haven't logged in for a specified period, list users who have been locked out, show accounts with expiring or expired passwords, and identify users with administrative privileges, display groups memberships.
  2. Group-Related Reports – The AD Security solution should list members of specific groups, show group memberships within groups.
  3. Security-Related Reports – The AD Security Solution should display security events and actions, show permissions and access rights for users and groups, identify potential security weaknesses.

7.1.7 IT Governance, Risk and Compliance (GRC)

- Currently Bank is using IT Governance, Risk and Compliance Solution.
- The bidder is required to Supply, Install, configure and maintain "IT Governance, Risk and Compliance" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure IT Governance, Risk and Compliance solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, IT Governance, Risk and Compliance Solution at DRC should act as Primary
- The proposed IT security Governance, Risk and compliance solution should be able to address the following key areas but not limited:
  1. Drive more value from internal audit management activities
     - Streamline basic audit processes with intuitive documentation
     - Increase audit efficiency with better planning and reporting
     - Improve business alignment with audit processes integrated with fraud management, process control, and risk management activities
  2. Effective, ongoing controls and compliance management. Focus resources on high impact processes, regulations, and risks to get continuous insight
  3. Preserve and grow business value with enterprise risk management. Understand what influences risk levels, how risks impact value, and which responses are most suitable with enterprise risk management.
  4. Include the following attributes: IT Security Risk Management, audit management, regulatory and compliance management, business continuity and 3rd Party risk management (or modules that cover the same subjects).
  5. All sub-modules must be relatable; i.e. centrally stored regulations should be accessible from each module; audit findings should be accessible in compliance/ERM modules, etc.
  6. Leverage Microsoft Office Products (particularly Word, Excel, and PowerPoint) to allow data and chart exports for external reporting needs and to allow current data to be migrated into GRC product to create baseline policy and procedures library as well as programmatic templates, etc.
  7. Help corporate boards, audit committees, executives, and operating managers:

    - Align risk management with business value drivers
    - Gain insight into how risks occur
    - Act on emerging risks and opportunities
  8. Scalable (capable of implementing one module/service at a time and adding users as needed).

- Bidder should integrate the proposed IT security GRC solution with the Bank‘s existing policies
- Bidder needs to ensure all existing compliance requirements of the Bank and other Banking regulatory bodies are incorporated
- Bidder is responsible for migration of all the data and policies from existing solution to the proposed solution.
- Sizing Guidelines for IT Governance, Risk and Compliance can be found in Annexure 2 - Minimum Technical Specifications, in the sub tab titles "Solutions Sizing".
- The IT Governance, Risk and Compliance solution should provide actionable reports, such as but not limited to below mentioned reports:
  1. Governance Reports - The IT GRC Solution should monitor adherence to organizational policies, track stakeholder engagement and satisfaction and measure the effectiveness of governance initiatives.
  2. Risk Management Reports - The IT GRC Solution should evaluate potential risks to the Bank, provides a centralized view of identified risks, their impact, and mitigation plans, monitor critical risk metrics and assess the effectiveness of risk mitigation strategies.
  3. Compliance Reports - The IT GRC Solution should track compliance with regulations and standards, manage audit findings and remediation actions, evaluate the effectiveness of internal controls, identify compliance gaps and remediation plans and assess the impact of new or modified regulations.
  4. Audit Reports – The IT GRC Solution should outline audit objectives and scope, document audit findings and recommendations and track progress on audit recommendations.

7.1.8 Decoy (Honeypot)

- Currently Bank is using Decoy (Honeypot) Solution.
- The bidder is required to Supply, Install, configure and maintain "Decoy (Honeypot)" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Decoy (Honeypot) solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Decoy (Honeypot) Solution at DRC should act as Primary

1. The proposed Honey Pot solution should be able to address the following key areas but not limited:
   1. Effectively create a replica copy of the Banks‘ existing internet-facing landscape
   2. Hacking incentive of the proposed decoy ecosystem should be as equivalent to present exposed incentive of the Bank
   3. The intended solution must safeguard the Bank against a target Reconnaissance attack, Lateral movement, Privilege Escalation, ransom ware and also act as a layer of defense for attacks based on new vulnerabilities, data theft and zero-day attacks
   4. Should provide real time Alerts
2. The solution should be able to integrate with the Active Directory

The Bidder is expected to implement the solution across the Banks' internet facing landscape and any other critical service as deemed by the Bank.

The bidder must integrate the honeypot solution with SIEM to generate alerts for any violations.

3. The primary responsibility of integration of solutions with existing SIEM lies with the Bidder selected through this RFP. The Bank shall provide adequate support to the Bidder for the purpose of integration.
4. Bidder should ensure the maintenance of the solution and provision of logs in integration with the SIEM for review with the Bank.
5. 24*7 monitoring of all the websites and services under the architecture of Honeypot with no exceptions
6. Bidder is responsible for migration of all the data and policies from existing solution to the proposed solution.
7. Sizing Guidelines for Decoy (Honeypot) can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
8. The proposed Decoy solution should provide a detailed view, such as but not limited to the below-mentioned telemetry:
    1. Attacker Behavior telemetry - The Decoy Solution should provide detailed information about the attacker, including IP address, geolocation, and attack techniques, identify common attack patterns and trends, analyze attack frequency over time and identify primary attack vectors used (e.g. Endpoint, web, network).
    2. Threat Intelligence - The Decoy Solution should detect security threats that might become initial attack vectors, leading to data breaches. It should also detect the well-known vulnerabilities and should have dynamic-ness to engage attackers.
    3. System Compromise - The Decoy Solution should detect signs of system compromise, identify attempts to steal data and detect attacker movement within the network
    4. Incident Response Reports - The Decoy Solution should provide a detailed chronology of attack events, documentation of mitigation steps and Automatic containment with 3rd party vendors

7.1.9 Mobile Device Management (MDM)

- Currently Bank is using Mobile Device Management Solution.
- The bidder is required to Supply, Install, configure and Maintain "Mobile Device Management" solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Mobile Device Management solution at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Mobile Device Management Solution at DRC should act as Primary
- The following elements are all required to construct a complete, end to-end mobility solution.
- Mobile devices, such as notebook PCs, tablet PCs, personal digital assistants (PDAs), Smart Phones, data and Internet services Infrastructure to support the application, especially next generation (4G) wireless networks and security/encryption software loaded on the mobile devices and network infrastructure Enterprise applications integration includes back office applications, legacy systems, security, and all the other aspects of Central Bank of India.
- The Mobile Device Management module is essential solution required by Bank to manage, monitor and support use of mobile devices.

- The proposed Mobile Device Management solution should be able to address the following key areas but not restricted:
    1. Configuration of the solution balancing critical document access requirements with data security assurance
    2. Tying mobility to strategic business objectives
    3. Identifies key business processes that can be improved with mobilization
    4. Defines business process improvements
    5. Devise business and technical alignment with Bank‘s requirement
    6. To implement every aspect of the identified and designed mobility initiative, including architecture and systems integration
    7. Assists with device management and configuration
    8. Provides different devices application hosting options
    9. Provides help desk services
    10. Scalable, so new users and increasingly sophisticated devices can be accommodated easily
- The bidder must provide training to the identified Bank personnel/ SOC team on the product architecture, functionality and the solution design – to be provided before the implementation of solution.
- Provide hands-on training to the Bank personnel/ SOC team on MDM policy configuration, alert monitoring, problem mitigation and etc. post implementation.
- The bidder must integrate MDM with SIEM to generate alerts for any MDM violations.
- The Bidder needs to ensure the proposed solution is configured to generate events for monitoring through SIEM
- Bidder is responsible for migration of all the data and policies from existing solution to the proposed solution.
- Sizing Guidelines for Mobile Device Management can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- The Mobile Device Management solution should provide actionable reports, such as but not limited to below mentioned reports:
    1. Device Inventory and Management Reports - The MDM Solution should provide detailed list of all managed devices with their specifications, assessment of device compliance with security policies, analysis of operating system versions across devices, detailed information about device hardware and installed software.
    2. Application Management Reports - The MDM Solution should provide list of installed applications on managed devices, assessment of application compliance with security policies and tracking of app deployment and updates.
    3. Security and Compliance Reports - The MDM Solution should evaluate device security status, identify compromised (Jailbroken / rooted) devices, assess password strength.

7.1.10 Secure Data Backup and Recovery (Ransomware Protection)

- The bidder is required to Supply, Install, configure and Maintain “Database Recovery and Ransomware Protection (Ransomware Protection)” solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Database Recovery and Ransomware Protection at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC.

In case of DR Drill or DC fails, Database Recovery and Ransomware Protection at DRC should act as Primary.

- Bidders is required to provide must provide “Database Recovery and Ransomware Protection” solution to protect ransomware / Cyber Attack or data corruption for Bank's Oracle Databases having following features
  1. The proposed Database Recovery and Ransomware Protection solution should support real -time data protection ensuring near zero data loss
  2. The proposed solution must be sized for Oracle Database to cater to the workload with minimum 500 TB of usable capacity.
  3. For detailed functional and technical specifications, refer to Annexure 2 – Minimum Technical Specifications
- The proposed solution must be sized for Oracle Database and other databases’ Workload with minimum 500 TB usable capacity
- Sizing Guidelines for Secure Data Backup and Recovery can be found in Annexure 2 - Minimum Technical Specifications, in the subtab titles "Solutions Sizing".
- The Secure Data Backup and Recovery (Ransomware Protection) solution should provide actionable reports, such as but not limited to below mentioned reports:
  1. Should show the status of ongoing and completed backups, identify backup failures and their causes, measure the time taken to recover data
  2. Provide unified dashboard showing Database recoverability status and protection policy for all source databases, with the ability to drill down further.

7.1.11 Network Access Control (NAC)

- The bidder is required to Supply, Install and Maintain “Network Access Control” solutions at Bank for the period of contract. The proposed solution is required to meet the technical specifications and bill of material given in Annexure 2 - Minimum Technical Specifications and Annexure 1 - Bill of Material.
- Bidder is required to configure Network Access Control at DC as Primary and at Disaster Recovery site as secondary, having high availability across DC and DRC. In case of DR Drill or DC fails, Network Access Control at DRC should act as Primary
- The Bank intends to procure a Network Access Control solution that should enforces policies to ensure only authorized and compliant users and devices can access Bank’s network.
- The proposed NAC Solution should provide below mentioned key features to enhance Bank’s network security:
  1. Endpoint Assessment: NAC should evaluate the security posture of devices attempting to connect to the network including wired and wireless network. It should include checking for antivirus software, firewall status, vulnerable application and operating system patches.
  2. Policy Enforcement: Based on the assessment results, NAC should enforce policies to allow, restrict, or deny access. Non-compliant devices may be quarantined or provided with limited access.
  3. Authentication and Authorization: NAC should verify the identity of users and devices before granting access. This should typically involve authentication methods like usernames/passwords, tokens, or biometrics.
  4. Guest Network Management: NAC should create and manage separate guest networks with restricted access, allowing for secure internet access for visitors or any other 3rd party user access.

5. Compliance Enforcement: NAC should help Bank to comply with Government regulations by ensuring that only authorized devices and users with the necessary permissions can access sensitive data.
6. Device Profiling: NAC should gather information about devices, such as manufacturer, model, and operating system, to identify potential security risks.
7. Network Visibility: NAC should provide visibility into all devices connected to the network, making it easier to identify unauthorized or compromised systems.
8. Threat Detection and Prevention: NAC should detect and prevent threats like malware, unauthorized access, and policy violations based on intelligence from the existing security solutions and block the assets automatically.
9. Integration with Other Security Tools: NAC should integrate with other security solutions, such as firewalls, IPS, EDR and SIEMs, to provide a comprehensive security posture.
10. Automation: NAC should automate many tasks, such as policy enforcement and device onboarding, to reduce administrative overhead.

- In case of failure of NAC appliance/ software, the Bidder shall provide redundant solution in no more time than 4 hours for any location wherever NAC is deployed.
- The Bidder is required to supply, implement & maintain NAC for:
    1. 36000 Endpoints (Includes DC, DRC, Branches. ATMs and Kiosks) and solution should be scalable to support 41000 endpoints during the period of contract.
    2. The solution is to be deployed at DC in HA mode and at DRC in HA mode.
    3. The NAC solution must Integrate with SIEM to generate alerts for any NAC violations.
    4. The responsibility of integration of solutions with existing SIEM lies with the Bidder selected through this RFP
    5. The Bidder needs to ensure the proposed solution is configured to generate events for monitoring through existing SIEM and EDR.
    6. The bidder/OEM must provide training to the identified Bank personnel/ SOC team on the product architecture, functionality and the solution design – to be provided before the implementation of solution.
    7. The bidder/OEM must provide hands-on training to the Bank personnel/ SOC team on NAC policy configuration, alert monitoring, and etc. post implementation.
- The Network Access Control (NAC) solution should provide actionable reports, such as but not limited to below mentioned reports:
    1. Device and User Activity Reports – The NAC solution should provide reports of user activity such as Logs of user logins, logouts, and network access attempts, including usernames, device information, and access times. The NAC solutions should also provide reports on the compliance status of devices based on predefined policies, including antivirus status, patch levels, and firewall configurations.
    2. Security Incident Reports – The NAC solution should provide reports on Security Alerts via notifications of potential security threats, such as malware detections, unauthorized access attempts, or policy violations.
    3. Compliance and Audit Reports – The NAC solution should provide Audit Trails with Logs of all administrative actions performed on the NAC system, including changes to policies, configurations, and user permissions.

4. Custom Reports – The NAC solution must allow for custom reports including Data Export with export of report data in various formats (e.g., CSV, PDF) for further analysis or integration with other systems.

7.2 Detailed Scope of work for Facility Management Services

- As a part of FMS, the Bidder shall provide services relating to maintenance and support of Security Solutions and associated hardware.
- The Bidder shall consider and envisage all services that will be required in the maintenance and the management of the Security Solutions.
- The services must meet the service levels mentioned in the RFP document.
- Bidder is required to perform the following below mentioned activities, but not limited to:
- Coordination of warranty repair or replacement service for Hardware and process warranty claims, as applicable. If the equipment is required to be taken outside the Bank premises, the cost of transportation and other related costs will be borne by the Bidder.
- Coordinating and scheduling maintenance activities with the End User and appropriate support functions of the Bank (e.g. network support, facilities support, etc.)
- Provision of recovery procedures to maintenance personnel of the Bank
- Maintain accurate documentation on the current location and status of Hardware in the process of being repaired
- Services including requirement analysis, assisting the YIL in hardware and system software platform acquisition, testing, verification, and installation. The Bidder accepts that these services allow access to business-critical software and also agrees that services provided include implementation and maintenance of the hardware as well as installation of the licensed software.
- Hardware maintenance services including preventive Hardware support, preventive maintenance, corrective maintenance to remedy a problem, and scheduled maintenance required to maintain the Hardware in accordance with manufacturers' specifications and warranties
- Provide maintenance data.
- Provide a single-point-of-contact to End Users for the resolution of Hardware related problems or to request an equipment upgrade or consultation. If the Hardware supplied by the Bidder is to be replaced permanently, then the Bidder shall replace the equipment of same Make/Model/configuration or of higher configuration.
- Provide support and assistance, as required, to isolate complex network, operational and software problems related to the proposed solutions and infrastructure
- Track and report observed Mean Time Between Failures (MTBF) for Hardware and/or software.
- Backup, remove, protect, and restore programs, data and removable storage media in a machine prior to presenting the machine for service
- Bidder is required to provide the following resources at the Bank premises to provide support as per the below table –

S. no	Time Window	No. of Resources
1	8 AM – 8 PM	6 x L1 Resources 2 x L2 Resources
2	8 PM – 8 AM	2 x L1 Resources

- Out of the resources mentioned above, 1 x L1 Resource in the 8 AM – 8 PM shift should have adequate experience in carrying out Red Team Exercise and should be able to carry out Red Team Exercises as and when required by the Bank.
- Resources must have back lining support with the OEMs of the proposed solutions to provide 24x7x365 support for the Bank's security solutions part of this RFP.

- L1 should have minimum 1 years of experience
- L2 should have minimum 4 years of experience
- Bank has the option to increase the number of L1 and L2 resources at the same rate quoted by the bidder for the duration of the contract.

8. General Responsibility of the Bidder

- For the Security solutions mentioned in the Bill of Material in Appendix 1, Bank has provided the minimum technical specification in Annexure 2.
- Bidders need to ensure that the solutions proposed are comply with these minimum technical requirements. The Bidder shall provide the sizing of the solution based on the information provided by the Bank in this RFP and Annexure 2 - of Minimum Technical Requirements. The Bidder shall provide the details of each individual solutions proposed along with the Hardware & software proposed, in Appendix 1 – Bill of Materials.
- Any components required for the successful implementation of the project should be the responsibility of the bidder.
- Bank is having EULA arrangement for Oracle. Accordingly, if the database proposed by the vendor is Oracle, no cost is to be mentioned. However, the license requirement should be clearly mentioned separately in the technical offer/document. If the proposed database is other than Oracle, the cost (original cost as well as ATS) should be mentioned and will be included in TCO.
- The Bidder shall provide the details of each individual solutions proposed along with the Hardware & software proposed in the RFP.
- Bidder should ensure dual power supply for all proposed solutions.
- Required racks, Network cables, and other component required for the successful implementation of the project should be the responsibility of the bidder. Bidder to provide the requirement at the time of bid submission.
- 42U Rack with dual PDU and perforated doors (600x800)
- All the equipment should be Rack Mountable and should have dual Power supply units.
- LTO8 Library based backup solution should be provided with backup software and necessary licenses. Feature online backup should be available.
- In case the bidder proposes any alternate solution in place of backup solution as mentioned above, they should be able to provide back up in removable device (tapes) to enable the bank for offsite storage of backup.
- The Bidder should take adequate care to avoid quoting security equipment that will become end of sale within 2 years of supply to the Bank and end of support within 7 years from the date of the submission of offer. In case any hardware / component reaches end of support during the contract period, bidder has to replace the same with new one, including successful installation and migration of data at no additional cost to the Bank. Failure to replace the product well in time by the actual end of support date will be treated as violation of SLA. Bank will procure new solution in such case and cost will be deducted from payables / payments as a penalty or by invoking PBG.
- The Bidder is required to procure, supply, install and provide subsequent comprehensive on-site warranty/AMC/ATS of the security equipment based on the Bill of Materials shared by the