

# PUNJAB & SIND BANK



## REQUEST FOR PROPOSAL

FOR

**SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION,  
MAINTENANCE & MANAGEMENT OF IT SECURITY SOLUTIONS - B**

**BID NO: PSB/HOIT/RFP/2025-26/45 DATED 01/10/2025**

## APPENDIX 1A: FUNCTIONAL

**HEAD OFFICE IT DEPARTMENT**

**2ND FLOOR,**

**PLOT NO. 151, SECTOR 44**

**INSTITUTIONAL AREA, GURUGRAM -122003**

| S. No | Solution Name  | Maximum Mark Obtained |
|-------|--|-----------------------|
| 1     | Information/Digital Right Management                   |                       |
| 2     | Centralized key management solution                    |                       |
| 3     | S-BOM & C-Bom  |                       |
| 4     | Database Activity Monitoring                           |                       |
| 5     | Mobile SDK   |                       |
| 6     | Identity & Access Management Solution                  |                       |
| 7     | Multi Factor Authentication                            |                       |
| 8     | Privilege Identity Management                          |                       |
| 9     | Information Technology, Government Risk and Compliance |                       |

#### Instructions

| Maximum Marks | Compliance (S/C)          | Maximum Mark  |
|---------------|---------------------------|---|
| 10            | <b>S (Standard):</b>      | This indicates that the requirement is covered by the standard product functionality. It includes features available out-of-the-box, as well as those achievable through parametrization or rules configuration.  |
| 6             | <b>C (Customization):</b> | Requirements marked as C (Customization) go beyond what is available or possible through standard product configuration. Customization involves:<br>Development of custom code<br>Creation of new functionalities or interfaces<br>Modifications that may impact upgrade paths or require specific deployment and testing cycles<br>User interface enhancements or custom-built screens<br>Creation of entirely new functionality not supported by the base product |

| S.No | Instruction  |
|------|--|
| 1    | Bidder must mandatorily mention the exact page number & clause or section reference from their submitted technical proposal or OEM product documentation which demonstrate compliance with each criteria (specification). Any Response marked as compliance without a valid page reference/section reference, shall be treated as in-complete and may be liable for rejection/scoring penalties  |
| 2    | Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product |
| 3    | All Regulatory guidelines requirements as on the date of Bid Submission should be complied from day 1. Bidder/OEM is also required to comply with all the guidelines (regulatory & statutory) issued during the contract period  |
| 4    | All the above mentioned features should be available form the day 1.   |

| DRM  |   |               |                  |         |
|------|---|---------------|------------------|---------|
| S.No | Required Functionalities/Features   | Maximum Marks | Compliance (S/C) | Remarks |
| A    | General   |               |                  |         |
| 1    | The solution is having capability to create and apply custom Rules at organization level, department level, Group level or user level as per requirements.  | 10            |                  |         |
| 2    | The solution is able to protect commonly used file formats like MS Office, PDF, CSV, Text, Text based formats, Open office formats, Image formats, RIF, .ZIP, .PPT etc.   | 10            |                  |         |
| 3    | The solution is capable to provide centralized monitoring, in build and custom reports of user activities and admin activities with capability of search option.  | 10            |                  |         |
| 4    | The solution is capable of assigning specific roles for monitoring of role-based document usage.  | 10            |                  |         |
| 5    | The solution is able to support databases like Microsoft SQL, Oracle, and MySQL etc. Bidder to provide comprehensive list of supported databases.   | 10            |                  |         |
| 6    | The solution is having integration capability with on-premises Windows Active Directory for user authentication and withdrawal of access rights if employee / onsite vendor staff left the organization / transfers.  | 10            |                  |         |
| 7    | The solution does not have any dependency on software from other vendor for its working.  | 10            |                  |         |
| 8    | The Solution is having integration capability with DLP (Data Loss Prevention) solution and able to apply Keyword based / File Classification based document protection.   | 10            |                  |         |
| 9    | The solution to support granular rights: viewing, copying, forwarding, editing, printing, screen capture prevention (even when file opens in native application), time-based expiry, and client type restrict access.   | 10            |                  |         |
| 10   | The solution is capable of rights retaining regardless of where files are stored, transmitted, used, and archived. Capable of applying rights and policies on the document irrespective of mode of document sharing i.e. SFTP, shared via One -drive, MS Teams, Share point, G-Drive, Dropbox, copied to USB etc. and should be independent of the collaboration platforms. | 10            |                  |         |
| 11   | The solution is capable of assigning Dynamic rights i.e. Rights can be withdrawn/ grant without recalling or resending the document to a specific User/ User group.   | 10            |                  |         |
| 12   | The solution is capable of allowing/ restricting Use/ access of documents, files by users, work groups, devices, IP etc.  | 10            |                  |         |
| 13   | Having capability to modify/revoke the document access post distribution, irrespective of the location of the document.   | 10            |                  |         |
| 14   | Having provision to add/delete users/policy on existing protected files which is already been shared.   | 10            |                  |         |
| 15   | The solution to deploy latest / strong encryption standards (AES 256) on Email/Documents/Other Files Formats. Bidder shall provide details regarding encryption/algorithm techniques being used in the solution.  | 10            |                  |         |
| 16   | The solution is having document protection capability on various devices i.e. desktops, laptops, tablets, iOS mobile devices fileservers and Android Mobile.  | 10            |                  |         |
| 17   | The solution is having capability of providing users (Internal/External) rights to access protected documents/ attachments using Android Mobile, IOS Mobile, and Browser.   | 10            |                  |         |
| 18   | View and Edit access to protected information is available on Desktops/Laptop browsers.   | 10            |                  |         |
| 19   | The solution provider is able to provide User Rights template with complete particulars.  | 10            |                  |         |
| 20   | The solution is capable of providing two factor authentication (such as OTP on Email for External user authentication) or integrate with third party authentication mechanism as per the requirement.   | 10            |                  |         |
| 21   | Solution should have workspace to share the files outside the organization without any dependency on the E-mail solution and shared drive being used by the Bank  | 10            |                  |         |
| 22   | The solution is having ability to dynamically Revoke access of a single user amongst all with whom a protected file is shared without any dependency on IRM client availability on that machine.  | 10            |                  |         |
| 23   | The solution including System/Appliance can address "single point of failure"; the failure of one or more components of the solution do not affect the organizational functionality in any way  | 10            |                  |         |

|    |  |    |  |  |
|----|--|----|--|--|
| 24 | The solution is capable of supporting segregation of duties, defining and assigning different user classes' i.e. End users, system administrators, policy administrators.  | 10 |  |  |
| 25 | The solution is capable to support delegation of duties and administrative functions for efficient management.   | 10 |  |  |
| 26 | The solution is able to distinctly handle external and internal users preferably through different user's directory.   | 10 |  |  |
| 27 | The Solution is supporting all MS Office versions offered by Microsoft and supports dominant MS Office formats (e.g., docx, doc, pptx, xlsx etc.) and pdf with advance permission controls.  | 10 |  |  |
| 28 | The external user is able to work i.e., READ and EDIT IRM protected documents as per the rights assigned by document owner.  | 10 |  |  |
| 29 | API is offered which can be integrated with Source systems/Vendor applications to apply/embed policy in the data for protection.   | 10 |  |  |
| 30 | The solution can provide Audit Trail with details of person using the document, location at which document is accessed, time & what has been done on the document.   | 10 |  |  |
| 31 | The solution does not require additional licenses for recipients of documents within or outside of the enterprise.   | 10 |  |  |
| 32 | The solution is having capability to have unique Identification and fingerprint assigned to each protected document. Which will be used to search / identify the document.   | 10 |  |  |
| 33 | The solution is having capability to protect documents and emails text during storage, transmission and while it is being used   | 10 |  |  |
| 34 | The solution is having capability to allow anyone to request access to a file directly from the file owner without any intermediary.   | 10 |  |  |
| 35 | The solution can be configured for allowing/ restricting access to specific devices/ machines, IP addresses, machines i.e., ability to restrict access of protected document inside and outside enterprise, can lock the information on a particular device. | 10 |  |  |
| 36 | The solution is supporting Virtualized environment for deploying server components.  | 10 |  |  |
| 37 | The solution is having capability for allowing access of protected documents to external authenticated users as per the rights assigned by the Document owner.   | 10 |  |  |
| 38 | The solution allows document creators to assign different rights for each user or group in the same window.  | 10 |  |  |
| 39 | The solution can be configured to impose dynamic document view protection like user-id watermark, jail-view and any other technology with Live timestamp, IP & mac address and print protection even when files are open in native application.              | 10 |  |  |
| 40 | The solution can enforce watermarked viewing of protected files even when the files open in native application.  | 10 |  |  |
| 41 | The solution can define and allocate roles & policies at System Administrator level. Document owner/Administrator should also be able to transfer document rights.   | 10 |  |  |
| 42 | Solution is providing basic troubleshooting capabilities at user machine that can be easily run by end users themselves.   | 10 |  |  |
| 43 | The solution having capability of sharing protected documents to external users via secure method.   | 10 |  |  |
| 44 | The solution provides off-line use of protected documents; can also control the period for which the user can have offline use.  | 10 |  |  |
| 45 | The endpoint client/agent should be easy to install and should provide for offline access to protected documents.  | 10 |  |  |
| 46 | The solution should support installation of endpoint client via standard desktop/infrastructure management tools.  | 10 |  |  |
| 47 | The solution should have capability of providing documents/ information security irrespective of vendor's/external users computing environment (Storage, Network Connectivity). This will be a fully offline environment.                                    | 10 |  |  |

|  |   |    |  |  |
|--|---|----|--|--|
| 48                                     | The solution is capable of providing possibility of Transferring/Replicating permissions to new document creator/owner/users in case previous document creator/owner/user has been transferred, on all the documents to facilitate user off-boarding and on-boarding. | 10 |  |  |
| 49                                     | The solution allows for automated folder-based protection in central file server.   | 10 |  |  |
| 50                                     | The solution is capable of providing enough protection even in case document formats are changed (e.g. Word file saved as html, pdf, etc.)  | 10 |  |  |
| 51                                     | The solution is capable of providing protected document recovery in case of cyber-attacks (ransom ware etc.)  | 10 |  |  |
| 52                                     | The solution is capable to provide end user the last updated protected documents as per owner directions.   | 10 |  |  |
| 53                                     | The solution is having capability of supporting Single/Multi mode authentication. The solution should be able to customize authentication based on user type (Internal/External)  | 10 |  |  |
| 54                                     | The solution should be such that there is no single point for unprotecting the documents other the document owner.  | 10 |  |  |
| 55                                     | The solution can support one or more methods applied on data such as password protection, auto-expiry, Geo/IP Fencing, biometric, Group policy to ensure greater control over sensitive data.   | 10 |  |  |
| 56                                     | The solution is having capability for supporting automatic deletion /disabling of internal and external users based on changes in Identity Sources.   | 10 |  |  |
| 57                                     | The solution is capable of establishing communication within the system as well as with external systems over secured communication protocols like https.   | 10 |  |  |
| 58                                     | The solution can allow authenticated users (external) to access (View/Print) protected documents with/without deploying agent   | 10 |  |  |
| <b>B Application Architecture</b>      |   |    |  |  |
| 59                                     | The architecture should support online real time updation between the application & database  | 10 |  |  |
| 60                                     | Integrity of the data should be maintained between the application & database.  | 10 |  |  |
| 61                                     | Proposed solution to provide SSO for login in to application & admin modules.   | 10 |  |  |
| 62                                     | Solution is capable and being offered in such a manner that includes installation either as a single instance or multi instance depending on Bank's requirements  | 10 |  |  |
| 63                                     | Capable of being implemented on a Centralized, localized and / or a hub and spoke model implementation  | 10 |  |  |
| 64                                     | Supports real time replication of data from production site to DR site and permit manual and automatic shift of the application to DR site  | 10 |  |  |
| 65                                     | Solution architecture has the capability to be configured in active-active mode   | 10 |  |  |
| 66                                     | Application supports database and OS level clustering   | 10 |  |  |
| <b>C Database Requirements</b>         |   |    |  |  |
| 67                                     | Ability to support for pooling multiple database connections when the load on the application increases   | 10 |  |  |
| 68                                     | Ability of the database to support clustering. Indicate the number of clusters that can be configured.  | 10 |  |  |
| 69                                     | Ability of the database to support central storage of data with multiple instances of the database  | 10 |  |  |
| 70                                     | The Database architecture should have the ability to increase the number of concurrent instances to keep the database server parameters utilization (CPU, Memory, Hard disk, etc.) within the defined threshold   | 10 |  |  |
| 71                                     | Ability to support online replication between DC, DR & NDR.   | 10 |  |  |
| 72                                     | Ability to implement SAN's for data storage in the architecture   | 10 |  |  |
| <b>D Hardware and Operating system</b> |   |    |  |  |
| 73                                     | The proposed Operating system should support IPV4 & IPV6  | 10 |  |  |
| 74                                     | Should be able to support different protocols (HTTP, HTTPS, TCP/IP, TLS, IPX, etc.)   | 10 |  |  |
| <b>E Security / Data Integrity</b>     |   |    |  |  |
| 75                                     | Integrity of data to be maintained at 100% of time  | 10 |  |  |
| 76                                     | Encryption to be used for data traveling between other interfaces   | 10 |  |  |
| 77                                     | System security is password controlled (for operating system, database, application and terminal id) which complies with the Bank's security policy (e.g. minimum password length, no. of attempts for logout, recycle of passwords etc.).                            | 10 |  |  |

|          |   |    |  |  |
|----------|---|----|--|--|
| 78       | sensitive data such as passwords and authentication credentials shall not be logged in transaction or system activity files   | 10 |  |  |
| 79       | The maximum data length for logging is pre-determined   | 10 |  |  |
| 80       | Successful and unsuccessful authorization events are logged   | 10 |  |  |
| 81       | An authenticated session, together with its encryption protocol, should remain intact throughout the interaction with the customer. In the event of interference, the application will ensure controls are in place to terminate the session and reverse out the affected transactions. As an integral part of the two-factor authentication architecture, appropriate measures to minimize exposure to a middleman attack which is more commonly known as a man-in-the-middle attack (MITMA), man-in-the browser attack or man-in-the application attack, are implemented. | 10 |  |  |
| 82       | Sensitive information that is passed in the cookies is encrypted.   | 10 |  |  |
| 83       | The session identifier shall be random and unique.  | 10 |  |  |
| 84       | The session shall expire after a pre-defined length of time.  | 10 |  |  |
| 85       | The Service Provider shall create adequate controls ensuring that, when exception or abnormal conditions occur, resulting errors do not allow users to bypass security checks or obtain core dumps  | 10 |  |  |
| 86       | The Service Provider shall only install or use cryptographic modules based on authoritative standards and reputable protocols (Please refer to the Customer's Cryptographic Key Management Guidelines). The Service Provider shall implement strong cryptography and end-to-end application layer encryption to protect end user's sensitive data in networks and storage. The Service Provider shall implement or support encryption during data transmission, delivery or couriered to external parties or other locations.   | 10 |  |  |
| 87       | Security framework is supported in terms of authentication, multi-level authorization, auto log-off, password control, single sign-on audit   | 10 |  |  |
| 88       | System allows administrators to implement access management in a granular manner  | 10 |  |  |
| 89       | System provides comprehensive audit trail features to monitor activity of specific programs and data files etc. The system should also provide on-line access to audit trail information including Time/date stamp, user ID, & before and after changes.  | 10 |  |  |
| 90       | Activities executed by the Application system administrator.  | 10 |  |  |
| 91       | Segregation of duties is permitted (e.g. segregated function between system and application administration)   | 10 |  |  |
| 92       | Ability to define groups so that access can be categorized  | 10 |  |  |
| <b>F</b> | <b>Interfaces</b>   |    |  |  |
| 93       | The system should be able to interface with Office365 & Outlook online and seamlessly.  | 10 |  |  |
| 94       | The system should be able to interface with MS Teams.   | 10 |  |  |
| 95       | The system should be able to interface with SharePoint.   | 10 |  |  |
| 96       | The system should be able to interface with OneDrive.   | 10 |  |  |
| 97       | Application to support various formats not limited to .pdf, .doc, .docx, .xls, .xlsx, .csv, .rif, .zip, .ppt, .eml & etc in applying security controls.   | 10 |  |  |
| 98       | The system should be integrated with DLP system of Bank.  | 10 |  |  |
| 99       | Interface able to handle exceptions (e.g. will output to log files, retries) when unsuccessful. Able to handle continual processing or gracefully terminated.   | 10 |  |  |
| <b>G</b> | <b>Audit Trail</b>  |    |  |  |
| 100      | Does the system provides comprehensive audit trail features such as:  |    |  |  |
| 100.1    | Daily activities log are merged into the history log files  | 10 |  |  |
| 100.2    | Date, time and user-stamped transaction list are generated for different transactions   | 10 |  |  |
| 100.3    | Do transaction screens display system information including Processing Date, Current Time, Current User   | 10 |  |  |
| 100.4    | Daily activity reports are provided to highlight all the transactions being processed during the day  | 10 |  |  |
| 100.5    | Support for recording of Unsuccessful attempts to log-in to the system  | 10 |  |  |
| 100.6    | System to provide session log files. The user should be able to analyze the information (e.g., account id, session time etc.)   | 10 |  |  |

|              |  |             |  |  |
|--------------|--|-------------|--|--|
| 100.7        | System should provide tracking of the client's IP & Network Interface address  | 10          |  |  |
| <b>H</b>     | <b>Reporting</b>   |             |  |  |
| 101          | Provide a full set of operational and audit trail reports for each of the modules.   | 10          |  |  |
| 102          | Periodical reports to appropriate authorities can be generated. The frequency and content of the reports can be determined by the bank user.   | 10          |  |  |
| 103          | 63 Generation / transmission of email alerts / advices at various stages of the transaction  | 10          |  |  |
| 104          | Support for online access of reports   | 10          |  |  |
| 105          | Ensure complete log of all successful/unsuccessful events/accesses to the system/database by users, resources used and actions performed (including recording all changed values where applicable) | 10          |  |  |
| 106          | Automatic report generation capability   | 10          |  |  |
| 107          | Pre-built query feature for non-programmers  | 10          |  |  |
| <b>I</b>     | <b>Archival and Restoration</b>  |             |  |  |
| 108          | Application should capable to archive and retrieval of history transaction.  | 10          |  |  |
| 109          | Application should capable to purge the history transaction.   | 10          |  |  |
| 110          | Purging & Archival should be automated process based on configuration at system/application level.   | 10          |  |  |
| <b>J</b>     | <b>Sizing</b>  |             |  |  |
| 111          | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. HA (Active/Active – N+N redundant Deployment) at DR<br>c. DR should be 100% replica of DC (Primary)                                   | 10          |  |  |
| 112          | Admin/Creator License for 200 user   | 10          |  |  |
| 113          | <b>Online Logs &amp; Data Storage</b> : 1 Month on primary storage and 2 months on Object Storage  | 10          |  |  |
| <b>Total</b> |  | <b>1190</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

| KMS    |   |               |                  |         |
|--------|---|---------------|------------------|---------|
| S. No. | Required Functionalities/Features   | Maximum Marks | Compliance (S/C) | Remarks |
| 1      | Key Manager platform should have the capability of Transparent Encryption for large-scale high-performance file system encryption   | 10            |                  |         |
| 2      | The Virtual form-factor of KMS should be FIPS certified (with certification in the name of the OEM)   | 10            |                  |         |
| 3      | The system should support an easy way to centrally store certificate and manage key and secret lifecycle tasks (generation, rotation, destruction, import and export) as per NIST 800-53, NIST 800-57   | 10            |                  |         |
| 4      | The system should support AES(128-256), ARIA,ECC(224-512), Brainpool curves, HMAC, SEED, TDES, RSA(512-4096) and the Crypto mode (CBC, CBC-CS1,ECB,GCM) etc.  | 10            |                  |         |
| 5      | The system should support API REST (JWT),SOAP, KMIP, PKCS#11, JCE, .NET, MSCAPI, MS CNG, C,NAE,XML, Java API's and libraries for integration with custom applications.  | 10            |                  |         |
| 6      | The System shall support Multi-tenancy using multiple domains, Clustering, High Availability and Backup.  | 10            |                  |         |
| 7      | The encryption of file/folders should be as per with FIPS approved & certified mechanisms & optionally, should not require any downtime while data encryption occurs.   | 10            |                  |         |
| 8      | Solution should be capable of determining application reading data and abnormal spike in I/O are notified and blocked from Encrypting Data thus providing ransomware protection   | 10            |                  |         |
| 9      | Solution should support Multi Factor Authentication (MFA) for users accessing protected path on Windows Servers   | 10            |                  |         |
| 10     | KMS should offer Block Cipher Encryption software providing encryption of File Servers (Windows/Linux) for data residing locally or for external attached storages, seamlessly integrated in a complex environment without changing the applications.   | 10            |                  |         |
| 11     | Solution must have the capability to identify "trusted applications" – binaries which are approved to perform encryption/decryption of business critical files.   | 10            |                  |         |
| 12     | The Block Cipher Encryption software should incorporate the encryption without having dependency on the native encryption capabilities of storage, database, cloud or Hypervisor. Well versed and adaptable with latest deployment technologies like Kubernetes, docker etc.  | 10            |                  |         |
| 13     | The Key Manager should offer various encryption and data discovery tools to locate the PII data in databases, images etc. captured by the web portal application giving a single glass pane view for centralized management.  | 10            |                  |         |
| 14     | The solution should be able to perform the secrets management capability(SSH,API keys, tokens), including but not limited to secrets of AWS, Azure, Docker ,Kubernetes and should support authentication methods like SAML, API key, Oauth etc.   | 10            |                  |         |
| 15     | The system should be configured to send e-mail notifications to specific addresses when system alarms are triggered.  | 10            |                  |         |
| 16     | The KMS should support Built in Data Discovery and Classification with both agent as well as agentless discovery of sensitive PII data using pre-built and customized templates including detection of data types within images with OCR feature. Scanning of large volumes of data, stored both on premise and in the cloud. This includes the scanning of local disks, network file shares, big data like Hadoop, as well as Cloud storage providers like AWS S3 and Azure Blob | 10            |                  |         |
| 17     | The KMS platform should support generation of keys from on premise HSM Key Source with the GUI to upload keys as Customer Managed keys to Public CSP such as AWS, Azure, Google, Oracle, SAP in order to maintain the complete ownership  | 10            |                  |         |
| 18     | The KMS Platform should be able to Integrate with provided HSM to master key in Hardware Root of trust and all should be from the same OEM.   | 10            |                  |         |
| 19     | The Bidder should support separate key management from CSP provider-controlled encryption; this key management component should be fully managed and owned by NIC. The Bidder shall support generation, storage and import/export of keys in BYOK scheme for multiple CSPs including: AWS, Azure, GCP, Oracle and Salesforce etc.   | 10            |                  |         |



|    |  |    |  |  |
|----|--|----|--|--|
| 20 | Should provide BYOE (bring your own encryption) for Multiple Databases like Oracle, PostgreSQL, MSSQL, MongoDB, SAP HANA etc. and Unstructured Data like PDF, log files etc. This BYOE option should provide strong transparent encryption and access control without the need of application modifications and no dependency on native encryption capability.   | 10 |  |  |
| 21 | The KMS should support data classification profiles based on current mandates Like GDPR, PCI DSS etc. The Data Discovery & classification should support Intelligent Remediation of discovered sensitive data by encryption  | 10 |  |  |
| 22 | The Solution supports capability to protect data through encryption or tokenization using a FIPS 140-2 level 3 compliant solution.   | 10 |  |  |
| 23 | Should support administrative interfaces like GUI, REST API, CLI, SNMP v1, v2c, v3, NTP, Syslog-TCP  | 10 |  |  |
| 24 | The Key Management solution must have KMIP support to enable the solution to store the encryption keys of solutions providing native encryption ensuring that even if the disk drives (physical or virtual) are stolen, the data stored within them remains protected against unauthorized access.   | 10 |  |  |
| 25 | The solution should have the capability to support bulk encryption and transformation from File to file , File to DB , DB to DB and DB to file   | 10 |  |  |
| 26 | The Proposed solution should be capable of Ransomware detection and blocking capability  | 10 |  |  |
| 27 | Network Management - SNMP, NTP, Syslog-TCP.  | 10 |  |  |
| 28 | Syslog Formats CEF, LEEF, RFC 5424   | 10 |  |  |
| 29 | API Support - • REST • KMIP • JCE, .NET, MSCAPI, MS CNG, API's and libraries for integration into custom applications.   | 10 |  |  |
| 30 | The bidder shall provide a comprehensive Key Management Solution that mandatorily includes Hardware Security Modules (HSM), appropriately sized based on customer requirements. The bidder will be solely responsible for the end-to-end delivery and functionality of the solution. In the event the proposed solution fails to meet the Bank's requirements, the bidder shall replace or upgrade it at no additional cost to the Bank. | 10 |  |  |
| 31 | HSM should be able to support : RSA(2048-8192), DSA, Diffie-Hellman, ECC ,ECDSA, ECDH, Ed25519, ECIES,, KCDSA, BIP32 (Digital Wallet Encryption), Milenage & Tuak (No separate license for algorithm)  | 10 |  |  |
| 32 | HSM should be able to support :AES, AES-GCM, DES, Triple DES   | 10 |  |  |
| 33 | Keys must remain securely inside the HSMs FIPS 140-3 Level3 validated cryptography boundary throughout the key lifecycle   | 10 |  |  |
| 34 | HSM should support Hash algorithms like : (Hash/Message Digest/HMAC): SHA-1, SHA-2, SHA-3, SM2, SM3, SM4   | 10 |  |  |
| 35 | HSM should have SP800-38F, SP800-108 Counter Mode  | 10 |  |  |
| 36 | Random Number Generation must comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A NIST 800-90B, NIST 800-90C compliant CTR-DRBG   | 10 |  |  |
| 37 | HSM must support minimum 5 cryptographically isolated partitions per device  | 10 |  |  |
| 38 | HSM must support the capability to run the custom code inside the HSM  | 10 |  |  |
| 39 | HSM must support Kyber key generation ,hash-based HSS, XMSS and XMSSMT (Multi-tree), and the Dilithium signing operations PQC algorithms   | 10 |  |  |
| 40 | HSM should have Protection against physical attacks through the monitoring of voltage and temperature (and abortion of any operation if voltage or temperature outside the expected range)   | 10 |  |  |
| 41 | HSM should have Detection of cover removal in addition to Alarm triggers for motion, voltage and temperature   | 10 |  |  |
| 42 | Security between HSM and the HSM client includes Message authentication  | 10 |  |  |
| 43 | Connections with HSM Client should terminate on HSM card and not on HSM chassis  | 10 |  |  |
| 44 | HSM should have FIPS 140-3 Level 3 security certification (with certification in the name of OEM)  | 10 |  |  |
| 45 | HSM must have CC EAL4+ on same appliance (with certification in the name of OEM)   | 10 |  |  |
| 46 | HSM must have UL, CSA, CE,FCC, CE, VCCI, C-TICK, KC Mark,RoHS2, WEEE,TAA,India BIS [IS 13252 (Part 1)/IEC 60950-1]   | 10 |  |  |
| 47 | SNMP, Syslog support and remote management capability  | 10 |  |  |
| 48 | HSM should support Windows, Linux, Solaris, AIX  | 10 |  |  |
| 49 | PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL and REST API for administration   | 10 |  |  |

|  |  |    |  |  |
|--|--|----|--|--|
| 50   | HSM must have Per-Key Authorization allows granular control of key material for applications requiring high assurance by providing authorization on a per-key basis.   | 10 |  |  |
| 51   | Only permitted IP can initiate SSH access to the HSM appliance   | 10 |  |  |
| 52   | HSM must support clustering of HSMs and load balancing without the need of external load balancer , The HSM should be capable of forming HA with existing HSM  | 10 |  |  |
| 53   | TCP/IP Network based appliance- 4 Gigabit ethernet ports with Port Bonding, out of box IPv4 and IPv6 support   | 10 |  |  |
| 55   | HSMs must be in Secure Transport Mode (STM), to ensure HSM have not been altered while in transit  | 10 |  |  |
| 56   | HSM should support the backup on FIPS certified hardware device, not to file in any form.  | 10 |  |  |
| <b>Certificate Lifecycle management (CLM)</b>  |  |    |  |  |
| The bidder, based on the architecture and design of their proposed solution, may choose to offer separate product for KMS and CLM. |  |    |  |  |
| 57   | The solution shall effectively manage the entire lifecycle of SSL/TLS certificates. This encompasses generation of Key using EAL4+ certified Certificate Manager, distribution, rotation, expiration, revocation, and archival processes, ensuring that cryptographic assets are appropriately managed throughout their lifecycle.   | 10 |  |  |
| 56   | The proposed solution shall provide secure certificate storage, as well as key and certificate lifecycle management for software-based keys used by hardware, appliances, operating systems, databases, hypervisors, virtual machines, network devices, virtual networks, middleware, web servers, application servers, application software, utility software, system software, and other technologies. It should also have the capability to integrate with public, private, and hybrid cloud environments, as well as container-based environments. | 10 |  |  |
| 56   | The solution shall support certificate management for all reputed operating systems, middleware, databases, web servers, application software, open source software technologies and utility software available in the market. e.g., Windows, Linux, AIX, HP-UX, Solaris, Apache, Oracle database and middleware products, IBM database and middleware products, NGINX etc. The solution should have the capability to integrate with public/private/hybrid cloud based and container-based environments as per the future requirements of the Bank.   | 10 |  |  |
| 56   | Use automation workflows to push certificates across multiple devices and Establishment of a unified trust anchor for issuing certificates across all OEM devices and applications   | 10 |  |  |
| 56   | The solution shall provide the facility to create templates of the key management workflows. The pre-defined templates for such process shall be provided as per the best practices across the globe.  | 10 |  |  |
| 56   | The solution should support SCEP, CMP, EST, and ACME protocols for automated certificate issuance. It must provide comprehensive API capabilities for integration with third-party systems. Additionally, the solution should be able to integrate with both public and private Certificate Authorities (CAs).   | 10 |  |  |
| 56   | The Certificate Lifecycle Management provider should be a Global Certificate Authority for SSL and Licensed CA authorized agency by CCA, Govt. of India and shall comply with existing and future Information Security Guidelines.   | 10 |  |  |
| 56   | In the Certificate Management, the solution should support automation of certificate renewal and provisioning to end devices. It should also support creation of the custom, event - driven automation workflows and tasks.  | 10 |  |  |
| 56   | The solution should provide capabilities for key and certificate discovery, vulnerability assessment, centralized inventory, certificate management and provisioning, as well as alerting, logging, and reporting. It should also include a powerful dashboard to monitor the status of all activities.  | 10 |  |  |
| 56   | Solution Should Continuous assessment to identify and remediate potential key and certificate-related vulnerabilities. Ability to manage access through blacklisting/whitelisting of devices, applications, and APIs.  | 10 |  |  |
| <b>Sizing</b>  |  |    |  |  |
| 57   | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. HA (Active/Active – N+N redundant Deployment) at DR<br>c. DR should be 100% replica of DC (Primary)   | 10 |  |  |

|              |   |            |  |  |
|--------------|---|------------|--|--|
| 58           | <b>Key Management Solution:</b> Enterprise wide licenses<br><b>Certificate Lifecycle management:</b> Enterprise wide licenses for Certificate Issuance, provisioning and management | 10         |  |  |
| 59           | <b>Online Logs &amp; Data Storage :</b> 1 Month on primary storage and 2 months on Object Storage   | 10         |  |  |
| <b>Total</b> |   | <b>680</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

| SBOM & CBOM |   |               |                  |         |
|-------------|---|---------------|------------------|---------|
| S. No.      | Required Functionalities/Features   | Maximum Marks | Compliance (S/C) | Remarks |
| <b>A</b>    | <b>Infrastructure, deployment and integrations</b>  |               |                  |         |
| 1           | The Services must be deployable in a production on-premises/on-premises. Private Cloud/India based public cloud/ Public-Private Hybrid India based Cloud environments.  | 10            |                  |         |
| 2           | The solution must correlate relevance of a vulnerability to a product based on data from VEX (Vulnerability Exploitability Framework)   | 10            |                  |         |
| 3           | The solution must provide integration with enterprise ticketing tools ( ITSM Manage Engine)   | 10            |                  |         |
| 4           | The solution must automatically close the vulnerabilities once the corresponding tickets are closed in the ticketing solution.  | 10            |                  |         |
| 5           | The solution must offer API for other parties to integrate and report vulnerabilities specific to a component or software application.  | 10            |                  |         |
| 6           | The solution must integrate with diverse vulnerability databases and advisories   | 10            |                  |         |
| 7           | The solution must support Single Sign-On (SSO) with the identity provider.  | 10            |                  |         |
| 8           | The solution must be able to integrate with AD to map the applications to application owners in the AD.   | 10            |                  |         |
| <b>B</b>    | <b>Functional and Technical Requirements</b>  |               |                  |         |
| 9           | The solution must align with CERT-In guidelines in terms of CBOM & SBOM requirements, generation, ingestion, updates and also cover software already running in the bank.   | 10            |                  |         |
| 10          | The solution must offer a portfolio view that pans across the entire footprint of applications being tracked in the bank.   | 10            |                  |         |
| 11          | The solution must offer a secure way of receiving CBOM & SBOM for third party vendor products through a vendor portal.  | 10            |                  |         |
| 12          | The solution must offer a secure way of exchanging CBOM & SBOM information by the bank with signing auditors or regulatory bodies.  | 10            |                  |         |
| 13          | The solution should recognize all packages via binary or dependency resolution via package managers.  | 10            |                  |         |
| 14          | Solution should be able to detect open-source packages and report related vulnerabilities, outdated versions, and license compliance risk.  | 10            |                  |         |
| 15          | Solution shall support out of box capabilities to execute scan against a public git repository e.g., Github   | 10            |                  |         |
| 16          | Solution should support integrations to CI servers e.g., Jenkins, Azure DevOps, gitlabs etc   | 10            |                  |         |
| 17          | The solution must support ingestion of CBOM (Cryptography Bill of Materials) & Software Bill of Materials (SBOM) through multiple channels, including: Direct upload via the tool's user interface Secure channel ingestion (e.g., API-based or encrypted transfer protocols) CI/CD pipeline integration with popular source code repositories such as GitHub, GitLab, and Bitbucket. | 10            |                  |         |
| 18          | The solution must offer an ability to track components for internal tools and third party tools.  | 10            |                  |         |
| 19          | The solution must be compliant with capturing the 21 fields against for components as per the CERT-In guidelines.   | 10            |                  |         |
| 20          | The solution must offer per product view into the known and discovered vulnerabilities.   | 10            |                  |         |
| 21          | The solution must be able to generate CBOM (Cryptography Bill of Materials) with following details:   | -             |                  |         |
| 21.1        | · Cryptographic Component/Module Name, e.g., OpenSSL, Bouncy Castle   | 10            |                  |         |
| 21.2        | · Library Name and Version, e.g., OpenSSL v1.1.1k   | 10            |                  |         |
| 21.3        | · Cryptographic Algorithm Used, e.g., AES, RSA, SHA-256   | 10            |                  |         |
| 21.4        | · Key Length, e.g., 2048-bit, 256-bit   | 10            |                  |         |
| 21.5        | · Protocol Name and Version, e.g., TLS 1.2, SSH 2.0   | 10            |                  |         |
| 21.6        | · Certificate Expiry Date, To track upcoming expirations  | 10            |                  |         |
| 21.7        | · Key Expiry Date / Rotation Schedule, If keys have a defined lifecycle   | 10            |                  |         |
| 21.8        | · Purpose of Use, e.g., encryption, signing, hashing, secure transport  | 10            |                  |         |
| 21.9        | · FIPS/NIST Compliance Status, Whether the crypto module is validated   | 10            |                  |         |
| 18.10       | · Location of Use   | 10            |                  |         |

|                                   |   |            |  |  |
|-----------------------------------|---|------------|--|--|
| 22                                | The solution must be able to scan and generate Cryptographic Bill of Materials (CBOM) & Software Bill of Materials (SBOM) for software deployments, based on a list of target machines provided by the organization.<br>This includes:<br>· Remote Discovery & Access: The tool should support remote access protocols (e.g., SSH, WinRM) or agent-based deployment to connect to each listed machine securely.<br>· Comprehensive Inventory Collection: It should automatically discover and catalog all installed software packages, libraries, and dependencies across various operating systems (Linux, Windows, etc.). | 10         |  |  |
| 23                                | The solution must be able to continuously monitor for known or discovered vulnerabilities for components and software in the bank and being tracked in SBOM manager.  | 10         |  |  |
| 24                                | The solution must support SBOM import/export in interoperable formats such as CycloneDX, SPDX and JSON.   | 10         |  |  |
| 25                                | There must be a single view of vulnerabilities from scanners, VAPT, bug bounty, etc. mapped to SBOM   | 10         |  |  |
| 26                                | The solution must provide a component level heatmap by profiling each software component within an application - based on known vulnerabilities, license issues or cryptographic asset weaknesses.  | 10         |  |  |
| 27                                | The solution must be able to map CVE age and severity to each application.  | 10         |  |  |
| 28                                | The solution must offer a risk level distribution by vulnerability classification   | 10         |  |  |
| 29                                | The solution must convey the data about licenses used by each component.  | 10         |  |  |
| 30                                | The solution must offer a risk level distribution by License classification (permissive, reciprocal and restricted)   | 10         |  |  |
| 31                                | The solution must be able to track application tags, ownership, lifecycle metadata for each application.  | 10         |  |  |
| 32                                | The solution must flag components nearing or beyond EOL/EOS, helping organizations proactively plan for upgrades or mitigation.   | 10         |  |  |
| <b>C Operations and Reporting</b> |   |            |  |  |
| 33                                | The solution must offer an ability to generate audit ready reports for consumption of auditors.   | 10         |  |  |
| 34                                | The solution must offer a Role Based Access Control that limits the view into data as per the roles configured in the system.   | 10         |  |  |
| 35                                | The solution must offer ability to view data by the application for each role base don certain fields.  | 10         |  |  |
| 36                                | The solution must support role based access like Auditor, Application Owner , Security Admin etc.   | 10         |  |  |
| 37                                | The solution must be able to generate, schedule and deliver reports over email for executives on a prescheduled cadence.  | 10         |  |  |
| <b>Sizing</b>                     |   |            |  |  |
| 38                                | a. Standalone at DC<br>b. Standalone at DR<br>c. DR should be 100% replica of DC (Primary)  | 10         |  |  |
| 39                                | Unlimited Application License   | 10         |  |  |
| 40                                | <b>Online Logs &amp; Data Storage :</b> 1 Month on primary storage and 2 months on Object Storage   | 10         |  |  |
| <b>Total</b>                      |   | <b>490</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

| DAM    |   |               |                  |         |
|--------|---|---------------|------------------|---------|
| Sr.No. | Required Functionalities/Features   | Maximum Marks | Compliance (S/C) | Remarks |
| 1      | The proposed DAM Solution should capture and analyze all database activities by application user, Database users and/or privileged user accounts, providing detailed audit trails that shows the "Who, What, When, Where, and How" of each database transaction.  | 10            |                  |         |
| 2      | The proposed DAM solution should help enterprises and financial institutions to address regulations such as GDPR, PCI-DSS, SOX, ISO 27701/27001, Data Privacy and organization specific policies by automating discovery and classification of sensitive data, assessing database vulnerabilities, recording database account activity, and producing compliance audit reports – at enterprise-class performance and scalability – across traditional RDBMS, Big Data architectures, and cloud database services. | 10            |                  |         |
| 3      | The proposed DAM solution should support the following authentication mechanism for accessing the solution:   | -             |                  |         |
| 3.1    | In-built authentication in the solution   | 10            |                  |         |
| 3.2    | Kerberos authentication   | 10            |                  |         |
| 3.3    | LDAP/AD authentication  | 10            |                  |         |
| 3.4    | RADIUS authentication   | 10            |                  |         |
| 3.5    | Support MFA authentication/token based/ SSO / IAM and Integration with PAM/PIM  | 10            |                  |         |
| 4      | The proposed DAM solution should enable segregation of duty in terms of account management, security administration and database administration.  | 10            |                  |         |
| 5      | The Proposed DAM Solution should support automatic updates to the signature database and based on global threat intelligence, ensuring complete protection against the latest threats.  | 10            |                  |         |
| 6      | The proposed DAM solution must be able to operate in FIPS (Federal Information Processing Standard) 140-2 compliance mode   | 10            |                  |         |
| 7      | The proposed DAM solution should integrate with 3rd party technologies like: SIEM, SOAR, Service Management, /Change Management, Ticketing system, Configuration Management (CMDB) tool etc. to provide holistic security posture (OEM Agnostic)  | 10            |                  |         |
| 8      | The proposed DAM solution should support more than in-memory database types including the categories of:  | -             |                  |         |
| 8.1    | Relational databases e.g. - MSSQL, My SQL and Oracle  | 10            |                  |         |
| 8.2    | Application in-built databases  | 10            |                  |         |
| 8.3    | Big Database types  | 10            |                  |         |
| 8.4    | Data lakes  | 10            |                  |         |
| 8.5    | Cloud based databases   | 10            |                  |         |
| 8.6    | Mongo-DB  | 10            |                  |         |
| 8.7    | Non-relational databases  | 10            |                  |         |
| 9      | Proposed DAM solution should have tiered architecture to provide to avoid any single point of failure and should have N+1 level of redundancy   | 10            |                  |         |
| 10     | The proposed DAM solution should have agent gateways and the solution should be offered as a Virtual Appliance.   | 10            |                  |         |
| 11     | The Advanced Data Security modules in DAM solution should be able to detect anomaly within the critical application processes based on behavior of the application and share real time alert to the Data Security solution.   | 10            |                  |         |
| 12     | The proposed DAM solution should support external storage such as SAN for increasing audit storage in future.   | 10            |                  |         |
| 13     | The DAM solution should support both agent-based mode and agentless mode to capture database activities.  | 10            |                  |         |
| 14     | DC & DR implementations should be centrally managed in DAM solution with a standard browser interface for management and monitoring   | 10            |                  |         |

|    |  |    |  |  |
|----|--|----|--|--|
| 15 | In the proposed DAM solution, if the communication between the agent and the gateway is lost due to agent mal-functions or uninstalled/disabled on server, immediate alert to be issued indicating the incident.   | 10 |  |  |
| 16 | In case of agent(s) based installation in DAM solution, it should not use the native database audit functionality. The agents should not employ native database transaction log auditing.  | 10 |  |  |
| 17 | Communication from Agent to management server must be encrypted in DAM solution.   | 10 |  |  |
| 18 | In case of agentless deployments, bidder to implement encryption between the log source and the DAM gateway or Server receiving Syslog connections at any given point in time.   | 10 |  |  |
| 19 | The proposed DAM solution should support, update of agents, configurations updates, policy updates, start/ stop/restart etc. at all the databases from management server centrally.  | 10 |  |  |
| 20 | The proposed DAM solution should provide CPU, RAM, disk capping capabilities on agent- based solution usually for agent-based system. The solution should not overload the network and delay real time monitoring and attack mitigation measures. Solution should have in-built capacity monitoring module and should support integration to any third-party Capacity Monitoring solution. | 10 |  |  |
| 21 | The proposed DAM solution must not use sampling and must capture every log ensuring the audit trail meets regulatory guidelines and standards of trust.  | 10 |  |  |
| 22 | The proposed DAM solution must have tamper-proof log storage capability to meet all compliance and regulatory requirements   | 10 |  |  |
| 23 | In The proposed DAM solution, audit policy and security policy should be mutually exclusive. The solution should be capable of generating security alerts even if an audit policy is not assigned to a given DB.   | 10 |  |  |
| 24 | The DAM solution should support integration of customized application database (where DB is in built- in application itself)   | 10 |  |  |
| 25 | The proposed DAM solution must monitor privileged user access or local SQL activity that does not cross the network such as Bequeath, IPC, Shared Memory, or Named Pipes   | 10 |  |  |
| 26 | The proposed DAM solution should be able to monitor in scope structured/semi structured database without dropping any event.   | 10 |  |  |
| 27 | The proposed DAM solution must support filtering/hiding of the bind variables of all the SQL activities captured   | 10 |  |  |
| 28 | The proposed DAM solution should provide information of DB links and should have capability to monitor the activity of DB links  | 10 |  |  |
| 29 | The customer should be able to deploy or remove the proposed solution from the network with no impact on the existing databases or the network architecture.   | 10 |  |  |
| 30 | The DAM agents should support Monitoring Mode and blocking Mode of Deployment. In monitoring mode, solution can generate alerts for unauthorized activity. In blocking mode, solution must proactively block the queries including blocking of matching signatures for known attacks like SQL injection.   | 10 |  |  |
| 31 | The proposed DAM solution should support creation of policies with multiple command groups, such that the number of rules/policies required to cover all type of queries are less.   | 10 |  |  |
| 32 | The proposed DAM solution should provide good compression ratio to store logs which will require minimum infra and should have ability to store the log online for multiyear retention requirement   | 10 |  |  |
| 33 | The proposed solution should have scale-out architecture to support any short or long surge of Transaction per sec. and it should not have repercussion on the licenses.   | 10 |  |  |
| 34 | The proposed DAM agents installed on DB should not need any additional users to be created in the DB   | 10 |  |  |
| 35 | The DAM solution should also discover any new/rogue database and DB objects created within the monitored network/systems and should send the real time alert to respective security staff  | 10 |  |  |

|      |   |    |  |  |
|------|---|----|--|--|
| 36   | The proposed DAM solution should be capable of auto discovering sensitive/confidential data like, credit card Numbers, Email address, Aadhaar numbers, PII, SPDI, guidelines in the database and offers the ability for customization.  | 10 |  |  |
| 37   | The proposed DAM solution should be able to auto discover privileged users in the database and should support user entitlement reviews on database accounts   | 10 |  |  |
| 38   | The proposed DAM solution should hold baseline discovery/classification/assessment results in the system, and it should be available as a reference for comparison for the new scan   | 10 |  |  |
| 39   | The proposed DAM solution should provide flexible methods to identify sensitive information based on the column details, data sampling and full scan  | 10 |  |  |
| 40   | The proposed DAM solution should be able to track both the application sessions and the database calls for applications and should identify the user session that was responsible for the given database call. It should support various platforms like .NET Core, .NET Framework, Nodejs, Java, Python etc.  | 10 |  |  |
| 41   | The proposed DAM solution should offer an option to not to save sensitive information in the audit logs   | 10 |  |  |
| 42   | Solution should be able to capture and monitor customized scripts like *.scr,*.sh,* .com  | 10 |  |  |
| 43   | Proposed DAM solution should monitor DDL, DML, DCL, TCL, DQL commands in real-time and it should also monitor user management, privilege management etc. and monitor for any policy violations.   | 10 |  |  |
| 44   | The Proposed DAM Solution should support custom security rules and support automatic triggering of alerts/SMTP notifications. Administrators should be able to define rules for the positive or negative security model and to create correlation rules with multiple criteria.   | 10 |  |  |
| 45   | The proposed DAM solution should allow policy definitions using very granular parameter like and not limited to: date and time, raw SQL, parameters used, end user name, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. and should offer to input any policy exceptions | 10 |  |  |
| 46   | The proposed DAM solution should inspect both in-coming and out-going DB traffic, compare with the rules and generate alert.  | 10 |  |  |
| 47   | The proposed DAM Solution should detect attacks on network protocols, operating systems, as well as application layer DB activity.  | 10 |  |  |
| 48   | The proposed DAM Solution should have capability to track execution of any Database Objects stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed.  | 10 |  |  |
| 49   | The proposed DAM solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.  | 10 |  |  |
| 50   | The proposed DAM solution should support correlated attack by examining multiple pieces of information at the network, protocol and application levels over time to distinguish between potential threats and valid user access behavior.   | 10 |  |  |
| 51   | The proposed DAM solution should have the ability to generate report showing the access of each user to the tables of each database along with the user who granted them the permission.  | 10 |  |  |
| 52   | The proposed DAM solution must support generation/both predefined as well as custom built reports as per customer requirements with both tabular views, pdf and data analysis graphical views. The solution should be able to generate the reports in PDF, Excel & CSV formats without developing or require lot of customization/changes from scratch.                     | 10 |  |  |
| 53   | The proposed DAM Solution must support either:  | -  |  |  |
| 53.1 | Ability to query raw event data via REST API  | 10 |  |  |
| 53.2 | Ability to perform bulk exports of raw event data, or   | 10 |  |  |
| 53.3 | Other external analytical and data store integration method.  | 10 |  |  |
| 56   | The proposed DAM solution should maintain the inventory of known IDS / IPS Signatures to be used in policies and detect the exploits in near real-time.   | 10 |  |  |



|       |  |    |  |  |
|-------|--|----|--|--|
| 57    | The proposed DAM solution should be capable of reporting missing patches from the database servers and report the details of such patches and vulnerabilities associated with. It should keep monitoring any such exploits and alert the stakeholders  | 10 |  |  |
| 58    | The proposed DAM solution should be able to virtually patch the known vulnerabilities automatically till a patch is installed for the same.  | 10 |  |  |
| 59    | The proposed DAM Solution should provide risk score of individual databases, based on combination of security alerts, discovery results, vulnerability assessment, sensitivity & confidentiality of data stored in the database.   | 10 |  |  |
| 60    | The proposed DAM Solution should have Risk Analytics   | 10 |  |  |
| 61    | The proposed Risk Analytics Solution should provide unified console which aggregates threat indicators across the enterprise data assets, including databases.   | 10 |  |  |
| 62    | The proposed Risk Analytics Solution should provide an intuitive dashboard page containing widgets that give a quick informative and drill down capabilities view of the following:  | -  |  |  |
| 62.1  | Protected Assets   | 10 |  |  |
| 62.2  | Open Issues  | 10 |  |  |
| 62.3  | Security Events Over Time  | 10 |  |  |
| 62.4  | Entities With Most Severe Incidents  | 10 |  |  |
| 62.5  | Events Analyzed  | 10 |  |  |
| 62.6  | System Health Status   | 10 |  |  |
| 63    | The proposed Risk Analytics Solution must be able to support the identification of anomalous activity based on DAM monitoring for databases including,   | -  |  |  |
| 63.1  | DB2  | 10 |  |  |
| 63.2  | MSSQL  | 10 |  |  |
| 63.3  | MYSQL  | 10 |  |  |
| 63.4  | Oracle   | 10 |  |  |
| 63.5  | Sybase ASE   | 10 |  |  |
| 63.6  | Teradata   | 10 |  |  |
| 64    | The proposed Risk Analytics Solution must be able to compress analyzed data  | 10 |  |  |
| 65    | The proposed Risk Analytics Solution must be able to differentiate between suspicious behavior from risky/abusive behavior (anomaly vs incident). It should be able to detect suspicious activity including scans for sensitive and valuable data, which may indicate the reconnaissance phase of a potential breach | 10 |  |  |
| 66    | The proposed Risk Analytics Solution should be able to access user's risk potential (compare user suspicious behavior rate to the rest of the organization and etc.)   | 10 |  |  |
| 67    | The proposed Risk Analytics Solution should automatically detect the following:  | -  |  |  |
| 67.1  | Nature of accounts which connect to the database (Service Account, DBA User Account. etc.)   | 10 |  |  |
| 67.2  | Purpose of database tables (Business Critical Tables, System Tables, and etc.)   | 10 |  |  |
| 67.3  | Data access habits (working hours, amount of data retrieved)   | 10 |  |  |
| 68    | The proposed Risk Analytics Solution must be able to detect Abnormal Behavior such as:   | -  |  |  |
| 68.1  | Database Access at Non-Standard Time   | 10 |  |  |
| 68.2  | Database Service Account Abuse   | 10 |  |  |
| 68.3  | Excessive Database Record Access   | 10 |  |  |
| 68.4  | Excessive Failed Logins  | 10 |  |  |
| 68.5  | Excessive Failed Logins from Application Server  | 10 |  |  |
| 68.6  | Excessive Multiple Database Access   | 10 |  |  |
| 68.7  | Machine Takeover   | 10 |  |  |
| 68.8  | Suspicious sensitive system tables scan  | 10 |  |  |
| 68.9  | Suspicious Application data access   | 10 |  |  |
| 68.10 | Suspicious Database command execution  | 10 |  |  |
| 68.11 | Suspicious Dynamic SQL activity  | 10 |  |  |
| 69    | The proposed Risk Analytics Solution must be able to identify/detect the following:  | -  |  |  |

|      |  |    |  |  |
|------|--|----|--|--|
| 69.1 | Typical end point information  | 10 |  |  |
| 69.2 | Typical database access patterns   | 10 |  |  |
| 70   | The Risk analytic engine must be able to scale-out in a large deployment environment to cater for the additional loads while maintaining a single management portal  | 10 |  |  |
| 71   | The proposed Risk Analytics Solution must be able to integrate with active directory and perform peer group analysis to enhance forensics. It should be able to provide line of sight into user identity.  | 10 |  |  |
| 72   | The proposed Risk Analytics Solution should provide context based on user information on AD which include the following widgets:   | -  |  |  |
| 72.1 | Employee Details with information such as email, phone numbers and office location   | 10 |  |  |
| 72.2 | Incidents which show a graphical view of the employee's number of incidents by severity  | 10 |  |  |
| 72.3 | Anomalies which show a graphical view of the employee's number of anomalies on a scale of Low to High  | 10 |  |  |
| 72.4 | Endpoints Activity which presents details on the number of endpoints that were used to access the resources by the employee  | 10 |  |  |
| 72.5 | Databases Activity which presents details on the number of databases that were accessed by the employee  | 10 |  |  |
| 73   | The proposed Risk Analytics Solution should be able to whitelist behavior which is authorized or acknowledge behavior that cannot be remediated immediately  | 10 |  |  |
| 74   | The proposed Risk Analytics Solution must be able to send syslog to SIEM or other Risk Analytics Solution for seamless incident management   | 10 |  |  |
| 75   | The proposed Risk Analytics Solution should automatically assign a Priority Score (a more granular threat score, on a scale of 1-100) to each incident for easier classification of important events   | 10 |  |  |
| 76   | The proposed Risk Analytics Solution must give incident details which should include Username, Source, Destination, Related/Correlated Issues, Type, Time, Severity and Priority. The Solution should include comprehensive incident details when investigating an incident, details should include: | -  |  |  |
| 76.1 | Description  | 10 |  |  |
| 76.2 | Severity Influencing Reasons   | 10 |  |  |
| 76.3 | Client and Server Details  | 10 |  |  |
| 76.4 | Incident Details   | 10 |  |  |
| 76.5 | Typical Behavior   | 10 |  |  |
| 77   | The proposed Risk Analytics Solution must be able to export detected incidents and anomalies to an excel file for offline review   | 10 |  |  |
| 78   | The proposed Risk Analytics Solution must be able to send email notification on detecting an issue/incident  | 10 |  |  |
| 79   | The proposed DAM solution should identify abnormal server and user behavior and provide early detection of possible attacks using outliners. For example:  | -  |  |  |
| 79.1 | User accessing a table for the first time  | 10 |  |  |
| 79.2 | User selecting a specific data in a table that he has never selected before  | 10 |  |  |
| 79.3 | Exceptional volume of errors   | 10 |  |  |
| 79.4 | Activity that itself is not unusual, but its volumes and time of activity is unusual   | 10 |  |  |
| 80   | Each gateway/controller must support at least 20,000 TPS irrespective of the type of query. The ability of gateway to support 20,000 TPS must not depend on whether the query is privileged query or a generic SQL Query.  | 10 |  |  |
| 81   | Proposed DAM should support database monitoring (both network and memory monitoring) with the combination of Solaris 11, with Processor Oracle Sparc M8 and Oracle T8-2 for Oracle 19 above. Banks CBS platform is already running on this setup.  | 10 |  |  |
| 82   | Each agent Gateway/cluster in the DAM solution should be able to process minimum 20,000 TPS (transactions per second) on an individual basis.  | 10 |  |  |

|      |   |    |  |  |
|------|---|----|--|--|
| 83   | The solution must have the capability to track the application users and the corresponding DB queries triggered to the backend DB server during the users' session.   | 10 |  |  |
| 84   | The DAM solution should support creation of policies/rules for enforcing access control and proper rights management on databases.  | 10 |  |  |
| 85   | The DAM solution should be capable of blocking access, real time execution of commands which violates the rule/ policies, store the events securely and report the same in real time.   | 10 |  |  |
| 86   | The DAM solution should have the ability to generate report showing the access of each user to the tables of each database along with the user who granted them the permission.   | 10 |  |  |
| 87   | Should provide a capability to enforce policies based on the compliance-controlled database [ Like PCI complied databases apply CC transaction and retrieval policy violations], group of databases, Database types like Oracle, MS SQL specific policies, locations like GDPR policies , Data protection policy for all DB's hosted], User Specific Policies | 10 |  |  |
| 88   | The DAM solution should support correlated attack by examining multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic   | 10 |  |  |
| 89   | The DAM solution should provide facilities for scheduling of reports with respect to time, type of activity, nature of event, violation of specific rules, user, source of origin, DB instance etc.   | 10 |  |  |
| 90   | The DAM solution should discover misconfigurations in the database and its platform and suggest remedial measures.  | 10 |  |  |
| 91   | The DAM solution should verify that default database accounts do not have a “default” password.   | 10 |  |  |
| 92   | The Risk Analytics Solution must give incident details which include Username, Source, Destination, critical Related/Correlated Issues, Type, Time, Severity and Priority   | 10 |  |  |
| 93   | The Risk Analytics Solution must be able to extract all available information on an incident directly   | 10 |  |  |
| 94   | The DAM solution should leverage AI/ML to:  | -  |  |  |
| 94.1 | Fine tune database users and their activities to raise alerts in case of any abnormality.   | 10 |  |  |
| 94.2 | Reduce false positives to minimum and raise only actionable and materialistic alerts.   | 10 |  |  |
| 95   | The DAM Solution shall have capability to automatically discover databases on the network and in the cloud infrastructure. It can automatically identify and classify sensitive data, using a number of techniques including dictionary and pattern-matching methods.   | 10 |  |  |
| 96   | License provided should support monitoring of Database installed on-premises, Private/public cloud also.  | 10 |  |  |
| 97   | License must be reusable and must not be bound to any onboarded Database servers and servers should be able to be removed from DAM to free up the licenses for other DB Servers.  | 10 |  |  |
| 98   | The DAM Solution for the following OS & DB combinations needs to be implemented and supported for all OS & DB Combination as and when implemented in the bank   | 10 |  |  |
| 99   | The DAM Solution should identify missing patches from the database servers  | 10 |  |  |
| 100  | The DAM solution shall help in monitoring of all local, network and application-level activities of the databases   | 10 |  |  |
| 101  | The DAM should prevent attempts to exploit known vulnerabilities  | 10 |  |  |
| 102  | The DAM verify that default database accounts do not have a “default” password  | 10 |  |  |
| 103  | The DAM Solution should be able to maintain logs for as per banks retention policy  | 10 |  |  |
| 104  | The DAM solution should run scheduled vulnerability scans for risk assessment and implement patches or apply virtual patches for all known vulnerabilities.   | 10 |  |  |
| 105  | The DAM Solution should be able to present vulnerability assessment findings in preconfigured reports for various compliance standard   | 10 |  |  |
| 106  | The DAM Solution shall allow the user to perform a fully automated discovery of all existing databases within the Banks environment.  | 10 |  |  |
| 107  | The DAM Solution should provide out-of-the-box reports which can be customized to meet regulations such as HIPAA, SOX, PCI DSS  | 10 |  |  |

|               |   |             |  |  |
|---------------|---|-------------|--|--|
| 108           | The DAM Solution should allow to create custom security policies based on the existing out-of-the-box policies and does the solution support the editing and creation of security policies that is driven by a user-friendly UI   | 10          |  |  |
| 109           | The DAM Solution should enable application of the policy across the entire environment on all the different types of databases deployed (MSSQL, Oracle, DB2, MySQL, etc.)   | 10          |  |  |
| 110           | The database agent monitoring Solution should possess the capability to conduct vulnerability scans and provide reports adhering to SANS 25, OWASP Top 10, and database-related CVEs, also be scan and adhering to compliance standards such as PCI DSS, DPDP etc. Integration with CVSS, NIST databases, and robust compliance reporting mechanism are also essential. | 10          |  |  |
| 111           | The DAM solution should be able identify data breaches by using the database audit  | 10          |  |  |
| 112           | The DAM solution should ensure that Hot Backups and Dump files are not readable   | 10          |  |  |
| 113           | The DAM Solution should support TLS-based encryption for comm. Between agent – management and vice versa.   | 10          |  |  |
| 114           | The DAM sol. Should offer functionality to monitor activity and access patterns within encrypted databases through secure integration/decryption methods.   | 10          |  |  |
| 115           | The DAM solution should be able to mask the sensitive and custom data in the audit logs.  | 10          |  |  |
| 116           | The DAM solution should identify and raise for data exfiltration.   | 10          |  |  |
| 117           | Proposed DAM should support database monitoring with the combination of Solaris 11, with Processor Oracle Sparc M8 and Oracle T8-2 for Oracle 19 above. Banks CBS platform is already running on this setup.  | 10          |  |  |
| 118           | The DAM solution should support custom/ inbuilt sensitive datatypes for the discovery and classification of data in database.   | 10          |  |  |
| <b>Sizing</b> |   |             |  |  |
| 119           | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. HA (Active/Active – N+N redundant Deployment) at DR<br>c. DR should be 100% replica of DC (Primary)  | 10          |  |  |
| 120           | Databases Count- 150 at DC and 150 at DR  | 10          |  |  |
| 121           | <b>Online Logs &amp; Data Storage</b> : 1 Month on primary storage and 2 months on Object Storage   | 10          |  |  |
| <b>Total</b>  |   | <b>1660</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have" shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

| Mobile SDK |  |               |                  |         |
|------------|--|---------------|------------------|---------|
| S. No.     | Required Functionalities/Features  | Maximum Marks | Compliance (S/C) | Remarks |
| 1          | Mobile App Security SDK to prevent the mobile app from running on Emulators & Simulators                                       | 10            |                  |         |
| 2          | Mobile App Security SDK to detect if the mobile app is running on a Jailbroken (for iOS) or Rooted (for Android) device        | 10            |                  |         |
| 3          | Mobile App Security SDK to detect Elevation of Privileges by the attacker  | 10            |                  |         |
| 4          | Mobile App Security SDK to detect if the mobile app is running on an outdated operating system                                 | 10            |                  |         |
| 5          | Mobile App Security SDK to identify if an android device has third party app store access enabled                              | 10            |                  |         |
| 6          | Mobile App Security SDK to detect if USB Debugging Mode and/or Developer Options are enabled on the android device             | 10            |                  |         |
| 7          | Mobile App Security SDK to detect Hooking Frameworks on Devices  | 10            |                  |         |
| 8          | Mobile App Security SDK to detect Device Screen Lock enablement  | 10            |                  |         |
| 9          | Mobile App Security SDK to enforce Device Policy as per business needs   | 10            |                  |         |
| 10         | Mobile App Security SDK to detect if the mobile app is running in a Sandbox environment  | 10            |                  |         |
| 11         | Mobile App Security SDK to detect if the mobile app is launched with the secondary profile on the Android device               | 10            |                  |         |
| 12         | Mobile App Security SDK to detect if mock location settings are enabled on the device  | 10            |                  |         |
| 13         | Mobile App Security SDK to detect time manipulation settings on the device   | 10            |                  |         |
| 14         | Mobile App Security SDK to prevent keystroke recording by malicious apps or keyloggers   | 10            |                  |         |
| 15         | Mobile App Security SDK to detect code injection attempts within the mobile application  | 10            |                  |         |
| 16         | Mobile App Security SDK to implement behavioral-based blacklisting of malicious devices  | 10            |                  |         |
| 17         | Mobile App Security SDK to detect if the mobile app is running on an unsecure Wi-Fi network                                    | 10            |                  |         |
| 18         | Mobile App Security SDK to identify a Rogue Access Point (RAP) when it is connected to the device                              | 10            |                  |         |
| 19         | Mobile App Security SDK to detect MiTM attacks   | 10            |                  |         |
| 20         | Mobile App Security SDK to monitor and prevent SSL Stripping   | 10            |                  |         |
| 21         | Mobile App Security SDK to detect fake certificates used for SSL decryption  | 10            |                  |         |
| 22         | Network threat detection function should be able to work without internet connectivity to app hosting servers                  | 10            |                  |         |
| 23         | Mobile App Security SDK to detect Proxy & VPN connections  | 10            |                  |         |
| 24         | Mobile App Security SDK to allow IP whitelisting for trusted VPN connections   | 10            |                  |         |
| 25         | Mobile App Security SDK to detect and defend against offline attacks by identifying when the device has no internet connection | 10            |                  |         |
| 26         | Mobile App Security SDK to prevent reverse engineering of the mobile app   | 10            |                  |         |
| 27         | Mobile App Security SDK to detect if the mobile app is being tampered  | 10            |                  |         |
| 28         | Mobile App Security SDK to prevent the attackers from decoding or modifying the business logic                                 | 10            |                  |         |
| 29         | Mobile App Security SDK to detect runtime recompilation or modification of an application                                      | 10            |                  |         |
| 30         | Mobile App Security SDK to detect if the App is not downloaded from trusted source - Play store and App Store                  | 10            |                  |         |
| 31         | Mobile App Security SDK to detect if the App is in Debug Mode  | 10            |                  |         |
| 32         | Mobile App Security SDK to detect if any blacklisted application is present on the mobile device                               | 10            |                  |         |
| 33         | Mobile App Security SDK to prevent Screen shot capturing   | 10            |                  |         |
| 34         | Mobile App Security SDK to prevent APK file Decompilation  | 10            |                  |         |
| 35         | Mobile App Security SDK to detect active screen mirroring during App usage   | 10            |                  |         |
| 36         | Mobile App Security SDK to detect App Spoofing Attacks when the App is launched  | 10            |                  |         |

|    |  |    |  |  |
|----|--|----|--|--|
| 37 | Mobile App Security SDK to detect side loading when the mobile app is launched   | 10 |  |  |
| 38 | Mobile App Security SDK should not collect any personal information from customer devices while protecting the Mobile App from malware. Therefore, malware protection should be based on <u>behaviour methodology and not on signature methodology</u> | 10 |  |  |
| 39 | Mobile App Security SDK to identify any overlay during App usage   | 10 |  |  |
| 40 | Mobile App Security SDK should work all the time as long as App is alive and active to protect from Malware threats, not just on the launch of the App   | 10 |  |  |
| 41 | Mobile App Security SDK to prevent Picture-in-Picture (PIP) Attacks and Draw over other App  | 10 |  |  |
| 42 | Mobile App Security SDK to identify Admin & Accessibility permission for Sideloaded Apps   | 10 |  |  |
| 43 | Mobile App Security SDK should comply with RBI DPSC guidelines   | 10 |  |  |
| 44 | Mobile App Security SDK should comply with OWASP Mobile Top 10   | 10 |  |  |
| 45 | Mobile App Security SDK should be able to support any device model having minimum Android version 8 or iOS version 12  | 10 |  |  |
| 46 | Mobile App Security SDK to notify the host application through callbacks in the event of device, network or malware-based threat detection   | 10 |  |  |
| 47 | Mobile App Security SDK should provide the API's to query the security state of the device by additional reference IDs already available with parent App system.   | 10 |  |  |
| 48 | Mobile App Security SDK should not collect any PII data from device or app   | 10 |  |  |
| 49 | Mobile App Security SDK should be able to allow for the usage of custom device identifiers and labels  | 10 |  |  |
| 50 | Mobile App Security SDK should be capable to execute detection of threats even if its System Control Portal is not reachable. Explain your approach on workings of detection and how threat data will be sent to console                               | 10 |  |  |
| 51 | Mobile App Security SDK to support React Native framework  | 10 |  |  |
| 52 | Mobile App Security SDK should provide the means of mapping the threat data detected with the actual user session or user id   | 10 |  |  |
| 53 | Mobile App Security SDK should comply with the security policies of Play Store and App Store, etc.   | 10 |  |  |
| 54 | Management Console Should integrate with SIEM/SOC platforms and provide all detailed threat forensic information   | 10 |  |  |
| 55 | Management Console should integrate with Fraud Prevention System   | 10 |  |  |
| 56 | Management Console should support Rest API's for integration with backend system   | 10 |  |  |
| 57 | Mobile App Security SDK to provide unique ref. or message ID on detection of each threat   | 10 |  |  |
| 58 | Mobile App Security SDK should have the capability to collect information of applications and processes running at the time of threat detection  | 10 |  |  |
| 59 | Management Platform should have option to deploy in High- Availability mode  | 10 |  |  |
| 60 | Mobile App RASP solution must be SDK based and there should not be dependency on Service provider for App version upgrades   | 10 |  |  |
| 61 | System Control Portal should be a web-based solution for configuration, integration and reporting of Mobile App RASP Solution  | 10 |  |  |
| 62 | System Control Portal should provide Role based access to console with proper segregation of group of users and functions.   | 10 |  |  |
| 63 | System Control Portal should provide details of No. of devices on which App is running on with breakup of Android and iOS devices.   | 10 |  |  |

|               |  |            |  |  |
|---------------|--|------------|--|--|
| 64            | System Control Portal should include details such as device OS version details, OS level threats detected, etc.  | 10         |  |  |
| 65            | System Control Portal should provide customizable Threat Policy configuration for different Apps   | 10         |  |  |
| 66            | System Control Portal should provide over the air updates for rule upgrades and configuration  | 10         |  |  |
| 67            | System Control Portal should provide statistics on Daily, Monthly Active devices   | 10         |  |  |
| 68            | System Control Portal should provide Dashboards highlighting change in trend of threats  | 10         |  |  |
| 69            | Service Provider should provide quarterly version updates  | 10         |  |  |
| 70            | Service provider should assist to close any code related vulnerabilities identified during VAPT or Code Review   | 10         |  |  |
| 71            | Service provider should undertake detailed Threat Modelling exercise before implementation of Mobile RASP solution   | 10         |  |  |
| <b>Sizing</b> |  |            |  |  |
| 72            | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. HA (Active/Active – N+N redundant Deployment) at DR<br>c. DR should be 100% replica of DC (Primary) | 10         |  |  |
| 73            | Users Count- 11,00,000 (Day 1) scalable to 25,00,000<br>Bsnk will procure additional license post utilization of 11,00,000 in tranches of 1,00,000               | 10         |  |  |
| 74            | <b>Online Logs &amp; Data Storage</b> : 1 Month on primary storage and 2 months on Object Storage  | 10         |  |  |
| <b>Total</b>  |  | <b>740</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

| IDAM   |   |               |                  |         |
|--------|---|---------------|------------------|---------|
| S. No. | Functional Specifications   | Maximum Marks | Compliance (S/C) | Remarks |
| A      | <b>Unified Identity Platform</b>  |               |                  |         |
| 1      | Unified identify platform should include automated identity intelligence, authentication, access, SSO, governance and lifecycle as part of the single unified platform  | 10            |                  |         |
| 2      | Proposed unified platform components (Authentication, SSO and IDAM) should be from a single OEM for seamless integration  | 10            |                  |         |
| B      | <b>Identity and Access Management (IDAM)</b>  |               |                  |         |
| 3      | The solution should have the capability to be easily deployed to rapidly connect to target systems with no scripting or coding required. The same UI should cater to all areas, including user interface, workflow design, access request, and application on-boarding (through pre-built out-of-the box adapters).                         | 10            |                  |         |
| C      | <b>Life Cycle Management</b>  |               |                  |         |
| 4      | For access via CLI (console, Telnet, SSH), WBM and Web Services (HTTPS) users can be authenticated via RADIUS/ TACACS+ or via local table of authorized users.  | 10            |                  |         |
| 5      | The solution should support provisioning/deprovisioning of users as well if the user ID of the users in the application is different from the user ID in the Active Directory.  | 10            |                  |         |
| 6      | Solution must have capability for creation of ticket / service / support ID/ Reference ID automatically or manually based on event or workflow. (ticket/Service / Support ID)   | 10            |                  |         |
| 7      | Solution must have capability to check duplication of User IDs and not allow creation of duplicate User IDs. (Duplication of user ids)  | 10            |                  |         |
| 8      | Solution must have capability for correlation and ability to merge user ID / identities in case where multiple identities are created for a single user. (User ID Merging)  | 10            |                  |         |
| 9      | Solution must be able to integrate with HRMS as Source system and integration with Active Directory and variety of business & technical applications (new-age, legacy, on-prem. and cloud with and without API's) as target system for user provisioning/de-provisioning. Bidder has to integrate all banks application with IDAM solution. | 10            |                  |         |
| 10     | Solution must have capability for configuration of workflow based on joiner, mover or leaver scenarios.   | 10            |                  |         |
| 11     | Solution must have capability for provisioning of users into variety of on-prem. and cloud based business applications  | 10            |                  |         |
| 12     | Solution should provide out of box integration with Finacle(CBS)  | 10            |                  |         |
| 13     | Solution should support modification of user's access based on transfer and promotions.   | 10            |                  |         |
| 14     | Solution must allow users to assign a delegate while away from the office for example, while on vacation. (Delegation of Authority)   | 10            |                  |         |
| 15     | Solution must act as Identity repository for users to know all type of access user having and eliminate the application-level user ID management. (Single User ID repository)   | 10            |                  |         |
| 16     | Solution must have capability for Provisioning and de- provisioning of users based on events such as approval and updation of all dependent target department.  | 10            |                  |         |
| 17     | Solution must allow to create/import user and their roles using manual (ex. csv) and automated interfaces.  | 10            |                  |         |
| 18     | Solution should support a 'least privilege' security model by decentralizing control with delegated administration.   | 10            |                  |         |
| 19     | User provisioning and de-provisioning should be possible in the Active Directory as well as in all applications (new-age, legacy, on-premises and cloud with and without API's).  | 10            |                  |         |
| 20     | The solution must support full lifecycle management of user's machine identities and access governance using cryptographic keys. This includes automated provisioning and deprovisioning to minimize the risk of credential sprawl and unauthorized access.   | 10            |                  |         |
| D      | <b>User Interface</b>   |               |                  |         |
| 21     | Solution must have a User-friendly Dashboard with Drag-and-drop interface with Guided wizard with dynamic reviewer dashboards and simpler setup and reviewer interface, with Rich UI for requesters, with context, risk, and SoD flags which shows risk insights inline during request,   | 10            |                  |         |



|          |   |    |  |  |
|----------|---|----|--|--|
| 21.1     | with Visual, event-driven workflow designer for easier visual workflow configuration  | 10 |  |  |
| 21.2     | with Localization & Accessibility for Better multi-language, responsive design support  | 10 |  |  |
| 21.3     | The same UI should cater to all areas, including roles simulation, workflow design, access request, Policies and application on-boarding  | 10 |  |  |
| <b>E</b> | <b>User Access &amp; Policy Review</b>  |    |  |  |
| 22       | Solution must have capability to review and certify user access periodically to ensure that users have the right access.  | 10 |  |  |
| 23       | Solution must have capability to highlight privileged user accounts and other high-risk accounts (e.g., service accounts, bots) during the certification process  | 10 |  |  |
| 24       | Solution must provide four different access certification campaign for periodic access review:  |    |  |  |
| 24.1     | Entitlement.  | 10 |  |  |
| 24.2     | Role Certification.   | 10 |  |  |
| 24.3     | Application/Owner Account.  | 10 |  |  |
| 24.4     | User Identity/Manager Account.  | 10 |  |  |
| 25       | Solution must have the capability to perform access reviews on an ad hoc or event-driven basis, such as when a user changes roles.  | 10 |  |  |
| 26       | Solution must have capability for a multi-step access review process so that more than one reviewer can verify the user access.   | 10 |  |  |
| 27       | Solution must provide governance administration capabilities integrate tightly with the provisioning solution so that any access that is denied is immediately revoked                                      | 10 |  |  |
| 28       | Solution must provide a single policy repository that is leveraged by all identity processes, including both detective and preventive access controls.  | 10 |  |  |
| 29       | Solution must automatically scan and detect policy violations.  | 10 |  |  |
| 30       | Solution must have capability to pull & generate reports in different logs format such as pdf and csv.  | 10 |  |  |
| 31       | Solution should be able to manage segregation of duties in applications.  | 10 |  |  |
| 32       | Solution must allow users to quickly and easily create a library of Separation of Duties (SoD) policies from the entitlements and access specific to our environment.                                       | 10 |  |  |
| 33       | Solution must support the ability to define and enforce access policies, including Separation of Duties (SoD) policies, between individual roles, between individual entitlements.                          | 10 |  |  |
| 34       | Solution must capture all activity information as part of audit logging & forward it to SIEM  | 10 |  |  |
| 35       | Solution must support for Public Key Infrastructure (PKI) and digital certificates to ensure legal non-repudiation during the login process, in compliance with the Indian IT Act                           | 10 |  |  |
| <b>F</b> | <b>Access Request</b>   |    |  |  |
| 36       | Solution must have capability to requests for access to applications that are not integrated for automatic provisioning, so that uniform request and approval processes can be applied to every application | 10 |  |  |
| 37       | Solution must have capability to enable the approver (manager, owner, etc.) to approve at a group or fine grained entitlement level.  | 10 |  |  |
| 37       | Solution must have capability to support end dates for when access should be granted on a temporary basis.  | 10 |  |  |
| 38       | Solution must support access request end-dates will remove the access whenever the approved time and date is reached.   | 10 |  |  |
| 38       | Solution must have capability to Automatically provision user access after access has been approved/authorized.   | 10 |  |  |
| 39       | Solution must have capability to identify users that have been provided access to systems directly by admins instead of by the IDAM solution.   | 10 |  |  |
| 39       | Solution must provide tools for identifying and managing orphan, rogue accounts   | 10 |  |  |
| 40       | Solution should have the capability to allow integration with 3rd party solutions via API.  | 10 |  |  |
| <b>G</b> | <b>General Requirement</b>  |    |  |  |
| 41       | Solution must run in a virtualized application environment such as VMware   | 10 |  |  |

|    |   |    |  |  |
|----|---|----|--|--|
| 42 | Solution must support bulk load mechanisms that can be used to quickly load data for users, accounts, services into the IDAM system.  | 10 |  |  |
| 43 | Proposed solution must be scalable to support future business growth  | 10 |  |  |
| 44 | Proposed solution must support clustering for load balancing and/or fail-over purposes  | 10 |  |  |
| 45 | Solution must support policies to enforce rules related to password complexity, expiry, length, password aging, password composition and password history enforcement. (Password policy)                                      | 10 |  |  |
| 46 | Solution must have capability for Synchronization of passwords across managed systems. (Password synchronization)   | 10 |  |  |
| 47 | Solution must integrate with Bank's privileged access management systems  | 10 |  |  |
| 48 | Solution must integrate with Bank's security information & event management (SIEM) solutions  | 10 |  |  |
| 49 | Solution must integrate with Bank's mail solution   | 10 |  |  |
| 50 | Solution must interface with various mechanism to push data into the solution and pull data out of the solution   | 10 |  |  |
| 51 | Solution must have single consoles for all features offerings: User life cycle management, Access request & Access Certification, Integration with Applications, Audit & Compliance Policy management & separation of duties. | 10 |  |  |
| H  | <b>Self-Service Access Request</b>  |    |  |  |
| 52 | Solution must provide self-service interface/module for users for additional access request   | 10 |  |  |
| 53 | Solution must have capability to allow users to manage their passwords and to reset a forgotten password without the help of an administrator.  | 10 |  |  |
| 54 | Solution must have capability to provide a page whereby users can view the current status of requests they have made to application administrators using the self-service interface   | 10 |  |  |
| I  | <b>Reports</b>  |    |  |  |
| 55 | Solution must support saving reporting results in downloadable file formats (e.g., PDF, Excel or CSV)   | 10 |  |  |
| 56 | Solution must include pre-defined reports out-of-the-box and pre-defined reports can be personalized by end users to fit their specific business needs  | 10 |  |  |
| 57 | Solution must provide report scheduler that allows user-specified reports to be run on a regularly scheduled basis and results can be automatically sent via email  | 10 |  |  |
| 58 | Solution must provide reports on Orphan Accounts and Policy violation   | 10 |  |  |
| J  | <b>Provisioning &amp; Connectivity Requirement</b>  |    |  |  |
| 59 | Solution must support account/access provisioning   | 10 |  |  |
| 60 | Solution must provide out-of-the-box provisioning connector with the solution   | 10 |  |  |
| 61 | Solution must provide custom connector development framework.   | 10 |  |  |
| 62 | Solution must provide manual provisioning capability (i.e. administrator-driven)?   | 10 |  |  |
| 63 | Solution must support retry if a transaction fails  | 10 |  |  |
| 64 | Solution must provide a toolkit for creating connectors for custom or homegrown applications  | 10 |  |  |
| K  | <b>Identity Analytics</b>   |    |  |  |
| 65 | Solution must support analytics capabilities to access the risk associated to the user and its access.  | 10 |  |  |
| 66 | Solution must provide recommendation for remediation action based on user's access like suspend/disable account or trigger access review request for user.  | 10 |  |  |
| 67 | Solution must provide comprehensive analytical reporting capabilities to assist with the cleansing of risky or excessive access   | 10 |  |  |
| 68 | Solution must provide a report which outlines defined security risks by application   | 10 |  |  |
| 69 | Solution must have capability to recommend risk mitigation actions for high-risk users, such as activity monitoring, ad hoc certifications, or remediation of policy violations   | 10 |  |  |
| 70 | Solution must have capability for assignment of unique risk values to each application, entitlement and role within the system  | 10 |  |  |
| 71 | Solution must have capability to track and monitor the risk of each user based on that user's access to sensitive applications and data (identity risk scoring)   | 10 |  |  |

|              |  |             |  |  |
|--------------|--|-------------|--|--|
| 72           | Solution must have capability to alert or notify managers, application owners or compliance officers based on changes to an identity or resource risk score  | 10          |  |  |
| 73           | Solution must provide dashboard with various insights like risky user, risky application, risky access, critical violation.  | 10          |  |  |
| 74           | Solution must notify responsible parties / application owner when policy violations are detected.  | 10          |  |  |
| 75           | Solution must able to generate, schedule, and view reports based on custom requirements. The solution shall provide out-of-box reporting templates to create one-time or recurring reports based on security events. | 10          |  |  |
| L            | <b>Role Mining</b>   |             |  |  |
| 76           | Solution must support both technical roles (Bottom-up) and business roles (top down) Role Modeling in GUI with graphical hierarchy support.  | 10          |  |  |
| 77           | Solution must support linking Business-to-Technical Role Mapping or entitlements with nested role views with context and complete provisioning capabilities  | 10          |  |  |
| 78           | Solution must have built-in Service on Demand enforcement so that it is embedded with policies, real-time conflict checks during role assignment.  | 10          |  |  |
| 79           | Solution must support advanced mining using access analyzer with usage clustering providing richer pattern detection from user behavior  | 10          |  |  |
| M            | <b>Single Sign-On (SSO)</b>  |             |  |  |
| 80           | Single sign on portal should get deployed fully on premise   | 10          |  |  |
| 81           | SSO portal must support multiple login mechanisms  | 10          |  |  |
| 81.1         | Two factor authentication  | 10          |  |  |
| 81.2         | Email authentication   | 10          |  |  |
| 81.3         | SMS authentication   | 10          |  |  |
| 81.4         | chain authentication (combining with AD password)  | 10          |  |  |
| 81.5         | one time link authentication   | 10          |  |  |
| 82           | SSO solution should have the capabilities to integrate with different applications using SAML protocol   | 10          |  |  |
| 83           | SSO solution should have the capability to include OIDC protocol if needed.  | 10          |  |  |
| 84           | The SSO solution can be installed in any OS provided (Linux or Windows)  | 10          |  |  |
| 85           | The administration of the solution must be protected by 2FA  | 10          |  |  |
| 86           | The SSO solution should have the capability to send audit logs to external syslog server   | 10          |  |  |
| 87           | The SSO solution must send verification emails to the users with any changes to his profile  | 10          |  |  |
| 88           | Enables users to log in everywhere with a single identity, and for administrators to manage access based on that identity  | 10          |  |  |
| 89           | It should be managed by identity management policy-based access decisions, ensuring that single sign-on (SSO) adheres to the organization's existing access management policies.                                     | 10          |  |  |
| N            | <b>Sizing</b>  |             |  |  |
| 90           | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. HA (Active/Active – N+N redundant Deployment) at DR<br>c. DR should be 100% replica of DC (Primary)   | 10          |  |  |
| 91           | Users Count- 12000 scalable to 14000   | 10          |  |  |
| 92           | <b>Online Logs &amp; Data Storage</b> : 1 Month on primary storage and 2 months on Object Storage  | 10          |  |  |
| <b>Total</b> |  | <b>1060</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

| IT GRC |   |               |                     |         |
|--------|---|---------------|---------------------|---------|
| S. No. | Required Functionalities/Features   | Maximum Marks | Compliance (Yes/No) | Remarks |
| 1      | The Solution should provide built in as well as customizable workflows to track, Legal compliance, IT RISK issues, third party risk management, Cyber threats, vulnerabilities, VAPT Findings, Audit Findings, Compliance findings, internal/external audits, critical incidents etc. | 10            |                     |         |
| 2      | The Solution should support advanced workflow capabilities such that multiple simultaneous paths/tasks and return back to earlier steps, phases or stages.<br>The workflow configuration should be driven via a graphical user interface.   | 10            |                     |         |
| 3      | The Solution should provide the ability to document, track, and monitor sign-off / approvals for any issues or actions.   | 10            |                     |         |
| 4      | The Solution should have option to store Content (policies, controls, report templates, reference documentation)  | 10            |                     |         |
| 5      | The Solution should allow users to filter and view policies by statically or dynamically defined criteria such as business unit, geography, impact area, role, etc.   | 10            |                     |         |
| 6      | The Solution should allow users to perform keyword searches to quickly find specific information among various IT / Accounts / Cyber Security and other policies as desired by PSB  | 10            |                     |         |
| 7      | The Solution should document the IT and Cybersecurity infrastructure including overview of business products/services, business processes, information assets, facilities and personnel and hierarchy of the Department.  | 10            |                     |         |
| 8      | The system should have surveys and questionnaires and automatically generate findings for incorrect responses.  | 10            |                     |         |
| 9      | The Solution should be able to manage the lifecycle of remediation plans, and it should also have the remediation action.   | 10            |                     |         |
| 10     | The Solution should be able to demonstrate control effectiveness metrics measurements in a comparable way against thresholds decided for metrics.   | 10            |                     |         |
| 11     | The Solution should have capability to use external data by having an API connection or any alternate connection method with the data source. The solution should also allow the importing the actual data in standard file format, such as csv, xls, etc.                            | 10            |                     |         |
| 12     | The Solution should have predefined assessment templates for global standards and allow and customizable assessment template as per PSB & GoI policies, standards, and other requirements.  | 10            |                     |         |
| 13     | The Solution should have pre- mapped controls for global standards and frameworks which include, ISO 27001/27002/27005/27032, CIS, COBIT, NIST, IT Act 2000/2008, GLBA, PCI DSS, SOX, ITIL v4.0.  | 10            |                     |         |
| 14     | The Solution should have the ability to document and maintain external benchmarks, frameworks, laws, and regulations identified for meeting the corporate objectives.   | 10            |                     |         |
| 15     | The Solution should offer a library of technical baseline configuration procedures mapped to various technologies.  | 10            |                     |         |
| 16     | The Solution should provide top- down or bottom-up approaches to developing key control procedures aligned with the compliance requirements as desired by PSB   | 10            |                     |         |
| 17     | The Solution should facilitate that Compliance requirements can be mapped to a business function  | 10            |                     |         |
| 18     | The Solution should have capability to record the consequences of non-compliance  | 10            |                     |         |
| 19     | The Solution should be able to calculate compliance scores as per standard, framework, regulation, department, including dynamically defined groups.  | 10            |                     |         |
| 20     | The Solution should have the ability to provide built-in assessments, Control Self Assessments (CSA) and questionnaires as well as manually create assessments and questionnaires per defined guidelines for conducting compliance testing  | 10            |                     |         |
| 21     | The Solution should support applying weight to questions and responses  | 10            |                     |         |
| 22     | The Solution should be able to collect and store the Management responses   | 10            |                     |         |
| 23     | The system should have the ability to define frequency of various review and reporting for outstanding issues and assigned task.  | 10            |                     |         |
| 24     | The Solution should have capability to perform gap analysis   | 10            |                     |         |
| 25     | The Solution should support risk assessments for both inherent and residual risk  | 10            |                     |         |
| 26     | The Solution should have the ability to document control activities and capture details like control owners, testing requirements, mapping with compliance, risk, business unit etc.  | 10            |                     |         |
| 27     | The Solution should be able to capture robust details about each risk item including objectives, products and services, business processes, risks, threats, vulnerability, impact, like hood controls, physical facilities, technology assets, policies, and procedures.              | 10            |                     |         |
| 28     | Risk assessments must have both qualitative and quantitative approaches.  | 10            |                     |         |
| 29     | The Solution should calculate, display, and report risk scores. Risk calculations must be transparent to users.   | 10            |                     |         |
| 30     | The Solution should give users full control over risk calculation parameters, weightings  | 10            |                     |         |
| 31     | The Solution should allow for aggregation of risks across the organization  | 10            |                     |         |
| 32     | The solution must keep the History of last 5 years risk   | 10            |                     |         |

|               |   |            |  |  |
|---------------|---|------------|--|--|
| 33            | The Solution should have the ability to capture and document risk response procedures as well as mitigating controls  | 10         |  |  |
| 34            | The Solution should have the ability to link, and map identified risk to Authoritative Sources, departments, asset, and divisions   | 10         |  |  |
| 35            | The Solution should be enabled to manage exceptions with appropriate risk sign-off/acceptance   | 10         |  |  |
| 36            | The Solution should provide the capability to document and capture details of stakeholders identified like asset owner, risk owner, control owners etc.   | 10         |  |  |
| 37            | The Solution should provide an out of the box risk register in order to capture currently maintained and tracked risks as well as ability to configure the application via no coding to accommodate our requirements.   | 10         |  |  |
| 38            | The Solution shall have capabilities to perform risk assessments as per risk category and/or threat category  | 10         |  |  |
| 39            | The solution should have capability to perform third-part risk assessment and should have ability to capture contracts and master services agreement associated with third party  | 10         |  |  |
| 40            | The Solution should have capability to define and automate the frequency of conducting the IT and Cyber Security risk assessment and automatically generating reports across various levels such as business unit head / manager, asset owner as well as board and management levels. | 10         |  |  |
| 41            | The Solution should include multiple impact categories to evaluate criticality of the business process  | 10         |  |  |
| 42            | The Solution should capture recovery time objective (RTO) and recovery point objective (RPO) for business processes and calculate the result as overall business criticality rating for the asset and/or process.   | 10         |  |  |
| 43            | The Solution should include workflow for multiple participants in the BIA (Business Impact Analysis) process, including the business process owner and others that may need to provide input, as well as review by another level and the relevant teams.                              | 10         |  |  |
| 44            | To support the BIA, the Solution should enable mapping of business processes to their supporting IT Service, Process, Third Party, and Personnel.   | 10         |  |  |
| 45            | The Solution should be able to generate report of ISO 27001 statement of applicability based on controls already existing or controls which are planned to be implemented.  | 10         |  |  |
| 46            | The Solution should be able to generate report on control effectiveness metrics for continual improvement of ISMS.  | 10         |  |  |
| 47            | The Solution should provide the ability to create a risk summary report that describes key risks, how they are being managed and monitored, remediation of key issues and accountability.   | 10         |  |  |
| 48            | The Solution should be able to generate report on Risk levels on risk assessment and risk treatment to showcase mitigation status   | 10         |  |  |
| 49            | The Solution should be able to generate risk treatment plan implementation progress report  | 10         |  |  |
| 50            | The Solution should be able to demonstrate open risk status with implementation progress, control gaps and assets affected  | 10         |  |  |
| 51            | The Solution should show dashboard including current audit findings, remediation, and responsibility.   | 10         |  |  |
| 52            | The Solution should be able to generate reports on audit findings, remediation, and responsibility  | 10         |  |  |
| 53            | The Solution should have options to display all the asset, risk, audit, action items and training related metrics in one single dashboard   | 10         |  |  |
| 54            | The Solution should provide a variety of layout options enabling business user to alter the user interface/dashboard  | 10         |  |  |
| 55            | The Solution should have capability to enable separate interface wherein vendor can login and provide response and upload artifacts   | 10         |  |  |
| 56            | The Solution should provide Enterprise risk management system and Enterprise Audit Management   | 10         |  |  |
| <b>Sizing</b> |   |            |  |  |
| 57            | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. Standalone at DR<br>c. DR should be 100% replica of DC (Primary)   | 10         |  |  |
| 58            | GRC Admin Users - 25 Scalable to 50   | 10         |  |  |
| 59            | <b>Online Logs &amp; Data Storage</b> : 1 Month on primary storage and 2 months on Object Storage   | 10         |  |  |
| <b>Total</b>  |   | <b>590</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

| Multi-factor authentication (MFA) |   |               |                  |         |
|-----------------------------------|---|---------------|------------------|---------|
| S. No.                            | Technical Specifications  | Maximum Marks | Compliance (S/C) | Remarks |
| 1                                 | The MFA solution must be support<br>-> On-demand authenticator (Short Message System)<br>-> Software authenticator<br>-> Hardware Authenticators  | 10            |                  |         |
| 2                                 | The proposed solution should be deployed completely on-premises without any dependency on cloud   | 10            |                  |         |
| 3                                 | The MFA authentication server must be available in hardware appliance or software form purpose built for 2FA Application by the OEM.  | 10            |                  |         |
| 4                                 | The MFA server must come with a RADIUS server with no additional cost.  | 10            |                  |         |
| 5                                 | The management interface of the RADIUS server must be fully embedded within the same management console as the MFA server to simplify setup and on-going management.  | 10            |                  |         |
| 6                                 | Solutions should be capable for integration with TACACS solution being used by the Bank.  | 10            |                  |         |
| 7                                 | The MFA server must support IETF RFC4758 (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required.   | 10            |                  |         |
| 8                                 | For access via CLI (console, Telnet, SSH), WBM and Web Services (HTTPS) users can be authenticated via RADIUS/ TACACS+ or via local table of authorized users.  |               |                  |         |
| 8.1                               | • 2FA server internal database  | 10            |                  |         |
| 8.2                               | • Latest Microsoft Active Directory   | 10            |                  |         |
| 9                                 | The MFA server must support multiple replicas when necessary without any additional cost and licenses   | 10            |                  |         |
| 10                                | MFA solution should Support FIDO and FIDO2 compliant Tokens   | 10            |                  |         |
| 11                                | The authentication agents must support the following platforms:   |               |                  |         |
| 11.1                              | Microsoft Windows<br>a. 32 Bit Platforms<br>• Windows Server<br>b. 64 Bit Platforms<br>• Windows Server   | 10            |                  |         |
| 11.2                              | Apache Web Server   | 10            |                  |         |
| 11.3                              | Red Hat Enterprise Linux  | 10            |                  |         |
| 11.4                              | IBM AIX   | 10            |                  |         |
| 11.5                              | Solaris   | 10            |                  |         |
| 11.6                              | SUSE Linux  | 10            |                  |         |
| 11.7                              | Oracle Linux  | 10            |                  |         |
| 11.8                              | Epic Hyperdrive   | 10            |                  |         |
| 11.9                              | Rocky Linux   | 10            |                  |         |
| 10.10                             | CentOS  | 10            |                  |         |
| 12                                | MFA solution must support on-premises deployment.   | 10            |                  |         |
| 13                                | The MFA server must be able to support software authenticators for the following platforms:<br>1. Smartphones<br>a. Android devices<br>b. iOS devices<br>c. Laptops and Desktops<br>d. Microsoft Windows & MAC OS | 10            |                  |         |

|              |  |            |  |  |
|--------------|--|------------|--|--|
| 14           | Solution should support adaptive authentication  | 10         |  |  |
| 15           | The 2FA solution should support or Integrate with cryptographic modules certified by FIPS 140-2 Level 2 & Level 3 for all cryptographic operations including the encryption of sensitive data at rest (password hashes, PINs, token records, etc.) and sensitive data in transit (server-to-browser, inter-server communication, etc.). All Agents used by the server should be compliant with the aforesaid | 10         |  |  |
| <b>A</b>     | <b>Self Service Module</b>   |            |  |  |
| 16           | Self Service portal must include the following functions:  |            |  |  |
| 16.1         | Authenticator Enrollment   | 10         |  |  |
| 16.2         | Request token  | 10         |  |  |
| 16.3         | Replace token  | 10         |  |  |
| 16.4         | Change/Set PIN   | 10         |  |  |
| 16.5         | Resync token   | 10         |  |  |
| 16.6         | Clear Security Questions   | 10         |  |  |
| 16.7         | Test Authenticator   | 10         |  |  |
| 16.8         | Report Lost Authenticator & Active Directory Password change and reset.  | 10         |  |  |
| 17           | The solution should have the capability to provide self service module and should provide the following  |            |  |  |
| 17.1         | • To provide intuitive, web-based interface to the users   | 10         |  |  |
| 17.2         | • Tool to determine if end-user is who they say they are and/or in possession of mobile device or Hardware token by performing Identity verification.  | 10         |  |  |
| <b>B</b>     | <b>Sizing</b>  |            |  |  |
| 18           | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. HA (Active/Active – N+N redundant Deployment) at DR<br>c. DR should be 100% replica of DC (Primary)   | 10         |  |  |
| 19           | Users Count- 12000 scalable to 14000   | 10         |  |  |
| 20           | <b>Online Logs &amp; Data Storage</b> : 1 Month on primary storage and 2 months on Object Storage  | 10         |  |  |
| <b>Total</b> |  | <b>380</b> |  |  |



| PIM   |  |               |                  |         |
|---|--|---------------|------------------|---------|
| S. No.  | Technical Specifications   | Maximum Marks | Compliance (S/C) | Remarks |
| <b>ARCON PAM (Privileged Access Management)</b> |  |               |                  |         |
| <b>A</b>  | <b>Lifecycle management</b>  |               |                  |         |
| 1   | The solution should have the capability to auto-onboard assets via integration with AD or bulk uploads (VM's, databases, network devices), groups, and discover accounts. It should be further able to configure rules to auto-assign the desired relationships/roles based on the least privileges.   | 10            |                  |         |
| 2   | The solution should have integration capabilities with Virtualization platforms, IaaS, and PaaS besides On-Prem AD/LDAP.   | 10            |                  |         |
| 3   | The solution should be able to onboard various systems including operating system accounts (Windows, Unix/Linux, Customized OS) and other infrastructure assets like Network devices, databases, application servers, etc.   | 10            |                  |         |
| 4   | The Solution Should support integration with devices like, Routers, Switches, Firewalls, UTM devices, NIPS, DDoS appliances, SIEM, HSM, WAF devices and Load Balancers for Web UI, GUI and CLI.  | 10            |                  |         |
| 5   | The solution should be able to integrate with a solution that provides a ready stack of APIs to help integrate with any HR or other such solutions that is the source of truth for identities within the organization.   | 10            |                  |         |
| 6   | The solution should be able to onboard the Organization structure from a directory store for ease of administration and be able to automatically onboard users into the privilege access management solution. The auto-onboarding capability should also be available for public cloud directories like AWS, Azure, GCP etc.                       | 10            |                  |         |
| 7   | The solution should have the capability to manage the Privileged Identity Lifecycle including certification/re-certification and governance for users, assets, and digital identities with built in review processes for all identities on the target systems.   | 10            |                  |         |
| 8   | The solution should include a challenge phase that allows users to re-verify their usage of privileged assets.   | 10            |                  |         |
| 9   | The solution should be able to identify orphan accounts on any target assets including auto-discovery of privileged accounts and reconciliation  | 10            |                  |         |
| 10  | The solution should be able to map privileged and personal accounts on various target systems  | 10            |                  |         |
| 11  | The solution should be able to identify private and public SSH keys, including orphaned SSH keys, on Unix/Linux machines, extracts key-related data, and ascertain the status of each key.   | 10            |                  |         |
| 12  | The solution should be able to manage Lifecycle of Human, Non-Human and Cloud Identities   | 10            |                  |         |
| 13  | The solution should be able to integrate with public cloud infrastructure.   | 10            |                  |         |
| <b>B</b>  | <b>Authentication &amp; Administration</b>   |               |                  |         |
| 14  | The solution should have the capability to integrate with any directory stores like Active Directory (AD) and Open LDAP or equivalent  | 10            |                  |         |
| 15  | The solution should provide an in-built directory store for local authentication with features of MFA authentication   | 10            |                  |         |
| 16  | The solution should provide features of SAML/OAuth/OIDC authentication as an identity consumer or identity provider.   | 10            |                  |         |
| 17  | The solution should have the capabilities to integrate with any adaptive or MFA authentication tools. It should support MFA integration at Vault user level as well as target device level from day one.   | 10            |                  |         |
| 18  | The solution should have their own built-in capabilities for adaptive and MFA especially the bio- metrics and mobile authenticators.   | 10            |                  |         |
| 19  | The solution should allow agile use of all or any authentication methodology at any given time.  | 10            |                  |         |
| 20  | The solution should provide a multi-domain authentication feature whereby the entire operations can operate in a distributed environment. This feature should be provided for authentication of users as well as Identity authentication for target systems.   | 10            |                  |         |
| 21  | The solution should allow the use of MFA to specific applications/portal and devices, systems based on the criticality of use.   | 10            |                  |         |
| 22  | The solution should provide ease of registration (for multiple MFAs) by end-users.   | 10            |                  |         |
| 23  | The solution should have an intuitive workspace wherein the access technologies for various applications or devices/systems should be auto on boarded and ready for use.   | 10            |                  |         |
| 24  | The solution should provide Browser based/ Native App workspace platform (browser- agnostic)   | 10            |                  |         |
| 25  | The adapters required for various technologies should be out of the box and for any unsupported technology the solution should provide a framework to build adapters   | 10            |                  |         |
| 26  | The solution should include a BOT builder/API for developing automated functions for transparent target connections, as well as any required dependencies, such as pre/post connection or manual input. For ease of integration, this is a necessity.  | 10            |                  |         |
| 27  | The solution should be able to ensure that the technology adapter can work in a multi- domain environment, that is, it should be able to authenticate multiple systems even if they operate in distributed authentication modes, such as multi-domain authentication.  | 10            |                  |         |
| 28  | For the best path of access, the solution should be able to handle multi-location architecture or distributed architecture with seamless integration at the user level. The solution should be able to intelligently route the user to the intended target system access in the safest possible way, considering simplicity of use and experience. | 10            |                  |         |
| 29  | A user should be able to submit JIT requests (Ephemerals accounts) for planned support, quick access, time- based access, or one-time access through the platform.   | 10            |                  |         |
| 30  | The solution should provide access to end-users based on least privilege principles. and then grant the user the ability to elevate users access based on certain roles and access approval methodologies with inbuilt dynamic workflows.  | 10            |                  |         |
| 31  | To ensure adequate segregation of duties, users on the access management system should be given role-based access.   | 10            |                  |         |

|      |  |    |  |  |
|------|--|----|--|--|
| 32   | To ensure that the solution is easy to manage it is imperative that the solution should have features for creating adequate roles for team leads, where in two/four eyes' principles are used for administration                                     | 10 |  |  |
| 33   | The PAM solution should provide Active Directory Bridging capability for *nix devices to connect with Active Directory.  | 10 |  |  |
| C    | <b>Workflow &amp; Notifications</b>  |    |  |  |
| 34   | The solution should have an inbuilt workflow to manage: -  |    |  |  |
| 34.1 | i) Electronic/Dual Approval based Password Retrieval   | 10 |  |  |
| 34.2 | ii) Onetime access / Time Based / Permanent Access   | 10 |  |  |
| 35   | Multi-level approval workflow with E-mail and SMS notification and delegation rules  | 10 |  |  |
| 36   | Ability to provide for the delegation at all levels in the workflow  | 10 |  |  |
| 37   | The solution should support a workflow approval process that is flexible to assign multiple levels of approvers based on product or model (i.e. require 2 or more approvals before access is allowed).   | 10 |  |  |
| 38   | The solution should support a workflow approval process that requires approvers to be in sequence before final approval is granted.  | 10 |  |  |
| 39   | The solution should support workflow delegation capabilities   | 10 |  |  |
| 40   | The solution should provide ready integration with service now for workflows   | 10 |  |  |
| 41   | The solution should have the capability to provide alerts and notifications for critical PAM events over SMS & Email   | 10 |  |  |
| 42   | The solution should have the capability to provide alerts and notifications for all administration/configuration activities over SMS & Email   | 10 |  |  |
| 43   | The solution should have the capability to integrate with other ITSM solutions for validating access.  | 10 |  |  |
| D    | <b>Session management, Logging and Reporting</b>   |    |  |  |
| 44   | Customizable notification for command executed on SSH and Telnet based devices   | 10 |  |  |
| 45   | The solution should be able to support a session recording of any session initiated via the session management solution including applications (desktop and web), servers (windows, *nix), network devices, databases, and virtualized environments. | 10 |  |  |
| 46   | The solution should be able to log commands for all commands fired over SSH Session and for database access.   | 10 |  |  |
| 47   | The solution should be able to record/log and search text commands for all sessions of the database even through the third-party utilities   | 10 |  |  |
| 48   | The solution should be able to record/log and search Keystrokes/text commands for all sessions on RDP  | 10 |  |  |
| 49   | The solutions should support search options for session-based recording on any combination of target account, group or target system and end-user.   | 10 |  |  |
| 50   | The solution logs all administrator and end-user activity, including successful and failed access attempts and associated session data (date, time, IP address, MAC as optional).  | 10 |  |  |
| 51   | The solution should be able to record old and new values for all logs related to the administrative activities within the solution   | 10 |  |  |
| 52   | The system should be able to define critical commands for alerting & monitoring purposes through SMS or Email alerts   | 10 |  |  |
| 53   | The solution should provide separate logs for commands and session recordings. Session recordings should be available in image/ video-based formats  | 10 |  |  |
| 54   | The solution should support secure and tamper-proof storage for audit records, policies, entitlements, privileged credentials, recordings, etc.  | 10 |  |  |
| 55   | The session recording should be SMART to help jump to the right session through the text logs  | 10 |  |  |
| 56   | The solution shall cater for live monitoring of sessions and manual termination of sessions when necessary   | 10 |  |  |
| 57   | The proposed solution shall support correlation by integrating with SIEM and unified auditing for shared and privileged account management/activity.   | 10 |  |  |
| 58   | Session management support in browsers using browser based with and without the need for the user endpoint to open an RDP, ssh, or local application   | 10 |  |  |
| 59   | The solution should offer RDP, SSH, or telnet protocol filtering (to detect, filter, or block specific commands or data)   | 10 |  |  |
| 60   | The solution should provide an extra layer of security especially on systems OS to provide access control on shared accounts and the ability to filter commands even if the rights are natively available to the share accounts.                     | 10 |  |  |
| 61   | The solution should be able to restrict usage of critical commands over SSH-based console based on any combination of target account, group or target system and end- user.  | 10 |  |  |
| 62   | The Solution should include workflow control while accessing critical assets like OS, DB, Network devices etc.   | 10 |  |  |
| 63   | The solution should restrict privileged activities on a windows server (e.g. host to host jumps, command/telnet access, application access, tab restrictions) from sessions initiated with PAM   | 10 |  |  |
| 64   | The solution should provide transparent connections to any target systems, including business applications and/or devices/systems (with or without passwords/ keys/ tokens).   | 10 |  |  |
| 65   | The solution should be able to establish a large number of concurrent connections from a secure gateway/Gateway that can also serve as a firewall for end-user applications, devices, and systems.   | 10 |  |  |
| 66   | Wherever applicable, technology adapters should be able to provide direct connections to end applications/systems/devices requiring the usage of a secured gateway/jump servers.   | 10 |  |  |
| 67   | The solution should support access to public cloud platforms and should allow transparent login to Cloud Management Consoles.  | 10 |  |  |

|          |  |    |  |  |
|----------|--|----|--|--|
| 68       | The solution should have the capability to launch enterprise applications (desktop and web) for admin access and their accesses should be monitored and logged.  | 10 |  |  |
| 69       | The solution should have the ability to grant role-based access to the target systems.   | 10 |  |  |
| 70       | The solution should provide out of the box reports for general daily operations  | 10 |  |  |
| 71       | The system shall have the ability to run all reports by frequency, on- demand, and schedule.   | 10 |  |  |
| 72       | The solution should provide detailed and scheduled reporting with the following basic report sets Entitlements Reports, User's activities, Privileged Accounts inventory and Activity log.   | 10 |  |  |
| 73       | The solution should have the ability to report on all system administrative changes performed by Access System Administrators with relevant auditable records  | 10 |  |  |
| <b>E</b> | <b>Security</b>  |    |  |  |
| 74       | The Solution should be TLS 1.2 and SHA-2 compliant for PCI-DSS compliance  | 10 |  |  |
| 75       | The Administrator user cannot see the data (passwords) that are controlled by the solution.  | 10 |  |  |
| 76       | The solution should secure master data, records, entitlement, policy data, and other credentials in a tamper-proof storage container.  | 10 |  |  |
| 77       | The solution should store Password and SSH keys safekeeping in the certified vault (minimum AES 256-bit encryption)  | 10 |  |  |
| 78       | The solution should support common protocols to connect to PAM servers to ensure the best interoperability with environments.  | 10 |  |  |
| 79       | The solution architecture should be highly scalable both vertically as well as horizontally.   | 10 |  |  |
| 80       | The solution should support multiple active instances with load balancing and fully automatic failover to another active instance  | 10 |  |  |
| 81       | The solution if required should be available to install on a virtual server  | 10 |  |  |
| 82       | The system should be highly available (24x7x365) and redundant from application failure, data failure.   | 10 |  |  |
| 83       | The solution should have the ability to integrate with enterprise authentication methods e.g. multiple 3rd party authentication methods including AD, LDAP, Windows SSO, PKI, RADIUS and a built- in authentication mechanism.   | 10 |  |  |
| 84       | The solution should have the ability to integrate with ticketing systems like Service Now, BMC Remedy etc.   | 10 |  |  |
| 85       | The solution should have ability to integrate with automation softwares for enhancing productivity in the data centre  | 10 |  |  |
| 86       | The proposed solution should supplied along with PAM soutuion that must supports integration with the Hardware Security Module (HSM) devices to store the encryption keys. And the proposed HSM should support atleast 500 tps RSA-2048 signing and 10 tps of RSA 2048 generation speed, with Supported symmetric & asymmetric encryption algorithms, Keys must remain securely inside the HSMs FIPS 140-3 Level3 validated cryptography boundary throughout the key lifecycle. Random Number Generation must comply with AIS 20/31 to DRG.4 using HW based true noise source alongside NIST 800-90A NIST 800-90B, NIST 800-90C compliant CTR-DRBG, HSM must support minimum 5 cryptographically isolated partitions per device . HSM must support Kyber key generation ,hash-based HSS, XMSS and XMSSMT (Multi-tree), and the Dilithium signing operations PQC algorithms | 10 |  |  |
| 87       | The solution should have the capability to detect/report/block and record outside PAM access   | 10 |  |  |
| 88       | The solution should have the capability to secure endpoints example: blacklisting, whitelisting of applications of the privileged users accessing the PAM solution which would provide a layer of defence.   | 10 |  |  |
| 89       | The offered PAM OEM Solution must be certified for Common Criteria Certificate EAL 2+ and supporting certificate document should be submitted during the bid submission.   | 10 |  |  |
| <b>F</b> | <b>Integrations</b>  |    |  |  |
| 90       | The solution should be able to integrate with leading SIEM solution like RSA Net Witness, QRadar, ArcSight, Splunk etc.  | 10 |  |  |
| 91       | The solution should be able to integrate with applications like VA Systems like Qualys, performance monitoring applications to eliminate hard-coded passwords  | 10 |  |  |
| 92       | The solution should have the capability to integrate with other IAM solutions and should provide SCIM compliant APIs.  | 10 |  |  |
| <b>G</b> | <b>Public Cloud Infrastructure and Entitlements Management (for Privileged Identities and Critical Data)</b>   |    |  |  |
| 93       | The solution should have the capability to discover and manage permissions and entitlements in the public cloud such as Azure, AWS, OCI etc  | 10 |  |  |
| 94       | The solution should provide centralized visibility and controls of permissions and entitlements across organizations public cloud.   | 10 |  |  |
| 95       | The solution should have the capability to monitor and identify any changes in the entitlement or permissions in real-time and report/notify of any inappropriate changes  | 10 |  |  |
| 96       | The solution should have the capability to provide suggestions or remediations to excessive privileges based on policies defined   | 10 |  |  |
| 97       | The solution should provide capability to provide Data Access Governance for various cloud drives like O365, Google Drive etc.   | 10 |  |  |
| 98       | The solution should be able to discover, govern users and entitlements for SaaS applications   | 10 |  |  |
| <b>H</b> | <b>Threat analytics</b>  |    |  |  |
| 99       | The solution should provide native analytics with AI/ML algorithms with identity threat protection capabilities.   | 10 |  |  |
| 100      | The solution should provide the ability to categorize risky users and their activities with a risk score based on AI/ML models.  | 10 |  |  |
| 101      | The solution should notify administrators when potentially harmful or suspicious activities occur.   | 10 |  |  |

|     |  |    |  |  |
|-----|--|----|--|--|
| 102 | The solution should use AI/ML techniques to detect anomalous activity without upfront human intervention.  | 10 |  |  |
| 103 | The solution should support analytics capabilities with self-learning nature to provide risk levels for user activities  | 10 |  |  |
| I   | <b>ARCON Secret Management</b>   |    |  |  |
| 104 | Secured Vault platform - main password storage repository should be highly secured (hardened machine, limited and controlled remote access, etc.)  | 10 |  |  |
| 105 | "The solution should provide a robust and mature vault to manage credentials, passwords, Keys secrets, certificates and such other artifacts as one would like to vault                                  | 10 |  |  |
| 106 | The solution should provide out of box connector integrating all standard systems (like HP tandem, Guardian etc.) to the Vault.  | 10 |  |  |
| 107 | The solution should provide for auto vaulting features as soon as the system is on- boarded.   | 10 |  |  |
| 108 | The solution should be able flexible to configure the policies and procedures of the organization, especially for passwords and secrets.   | 10 |  |  |
| 109 | The solution should provide features to create local or general exceptions to the rules or policies.   | 10 |  |  |
| 110 | The solution should be able to provide rotation capabilities at scale (across technologies)  | 10 |  |  |
| 111 | The solutions should be able to create a sequence or automate events or actions based on technology requirements to ensure that any rotation activity is conducted without any manual intervention       | 10 |  |  |
| 112 | The solution should be able to provide features for JIT (Just in time), on-demand, and time-based rotations of passwords   | 10 |  |  |
| 113 | The solution should be able to automatically sync any out of sync passwords without using any external utilities (on target systems/applications)  | 10 |  |  |
| 114 | A single person/user should not be able to check out any credentials, always two or four eyes' principles should be applied  | 10 |  |  |
| 115 | Offline access of managed credentials in case of vault failure should generate audit logs that are synced with the Vault once it's back online (break glass facility).                                   | 10 |  |  |
| 116 | The solution should provide a high-velocity vault that is agile and dynamic to generate not only unique passwords/secrets but also unique credentials especially for cloud assets that are auto-scaled   | 10 |  |  |
| 117 | The solutions should be able to onboard and support credential management for cloud and containerized environment  | 10 |  |  |
| 118 | The solution should provide a secure method to facilitate access to managed assets in case of PAM failure for identified users (local vault) like fail safe features                                     | 10 |  |  |
| 119 | The solution should have a central administration console for unified administration   | 10 |  |  |
| 120 | The PAM solution must have the capability of secrets management (passwords, PINs, Application passwords, certificates, SSH keys etc) and from day 1 it should maintain at least 50 application passwords | 10 |  |  |
| J   | <b>Reports and Dashboards</b>  |    |  |  |
| 121 | Must be able to provide comparative pre-defined reports and capable of producing customized  | 10 |  |  |
| 122 | Must be able to distribute reports on demand and automatically (based on defined on schedule)  | 10 |  |  |
| 123 | Must allow bulk downloads of the reports as and when required.   | 10 |  |  |
| 124 | Must be capable of providing remediation advise  | 10 |  |  |
| 125 | Must be able to provide a dynamic dashboard to review the risk @360 view. Further, the dashboard must have the capability to drill down to the lowest level of control risk.                             | 10 |  |  |
| 126 | Must be capable of customizing the dashboard as per requirement  | 10 |  |  |
| 127 | The solution should support notifications on email, UI, etc.   | 10 |  |  |
| K   | <b>Business as Usual behavior</b>  |    |  |  |
| 128 | Must be able to archive and restore data   | 10 |  |  |
| 129 | Must not require a reboot after installation/configuration   | 10 |  |  |
| 130 | The audited data transfers should be through an Encrypted channel  | 10 |  |  |
| 131 | Must be able to capture before and after snapshot of configuration data.   | 10 |  |  |
| L   | <b>User Management</b>   |    |  |  |
| 132 | Solution must provide an option to provide authorization to the users  | 10 |  |  |
| 133 | Must provide user provisioning system  | 10 |  |  |
| 134 | The solution shall allow to modify the asset inventory as per requirement  | 10 |  |  |
| 135 | Solution must be able to integrate with AD/LDAP directories  | 10 |  |  |
| 136 | The solution must provide local authentication mechanism.  | 10 |  |  |
| 137 | The security administrator console must be able to support 2-factor authentication   | 10 |  |  |
| 138 | The solution should provide RBAC-based access to the users. The RBAC should be granular based on the devices/systems.  | 10 |  |  |
| M   | <b>Data Security</b>   |    |  |  |
| 139 | Must provide data protection and encryption solution   | 10 |  |  |
| 140 | The security administrator console must be able to support 2-factor authentication   | 10 |  |  |

|              |  |             |  |  |
|--------------|--|-------------|--|--|
| 141          | Support industry proven cryptograph security standard: AES 128, 256-bit cipher and asymmetric key RSA-4096/2048, SHA-256 algorithm   | 10          |  |  |
| 142          | The proposed solution must support multi-tenancy using separate domain with configurable policies, data encryption key management and audit log  | 10          |  |  |
| <b>N</b>     | <b>Deployment Transparency</b>   |             |  |  |
| 143          | Must be able to support transparent deployment which does not require application code change  | 10          |  |  |
| 144          | Must be able to support deployments including physical, virtual, and cloud-based servers with minimal administrative overhead  | 10          |  |  |
| 145          | The solution should allow hybrid deployment which involves cloud to cloud, cloud to on-prem and on-prem to cloud scanning of the assets.   | 10          |  |  |
| 146          | The solution shall avoid multiple port openings between itself and the target assets from a security perspective.  | 10          |  |  |
| 147          | Must be able to support a centralized policy with highly configurable security and policy enforcement to provide granular access control and audit   | 10          |  |  |
| 148          | Must be able to work in a distributed environment  | 10          |  |  |
| 149          | Must support multiple databases for deployment.  | 10          |  |  |
| <b>O</b>     | <b>High Performance</b>  |             |  |  |
| 150          | The proposed solution should have minimum performance impact on target server with not more than 10% performance overhead.   | 10          |  |  |
| 151          | The proposed security repository must support high-availability clustering configuration across LAN and WAN. Vendor must provide network architecture diagrams to illustrate the high availability setup                   | 10          |  |  |
| 152          | Must have a single console and the scan connections should be seamless.  | 10          |  |  |
| 153          | Solution shall support concurrent assessments of multiple technologies.  | 10          |  |  |
| <b>P</b>     | <b>Sizing</b>  |             |  |  |
| 154          | a. HA (Active/Active – N+N redundant Deployment) at DC<br>b. HA (Active/Active – N+N redundant Deployment) at DR<br>c. DR should be 100% replica of DC (Primary)   | 10          |  |  |
| 155          | User Licenses : 500 User (Day 1) scalable to 750<br>Services Licenses - 2500 service (Day 1) scalable to 3000<br>License to Access Vcenter - 25 (Day 1) Scalable 50  | 10          |  |  |
| 156          | a. Online Logs & Data Storage 1 Month on primary storage and 2 months on Object Storage<br>b. All Videos should be stored on Object Storage for 3 Months periods post which it should backed up as per the backup policies | 10          |  |  |
| <b>Total</b> |  | <b>1570</b> |  |  |

Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or "Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product

# PUNJAB & SIND BANK



## REQUEST FOR PROPOSAL

FOR

SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION,  
MAINTENANCE & MANAGEMENT OF IT SECURITY SOLUTIONS - B

BID NO: PSB/HOIT/RFP/2025-26/45 DATED 01/10/2025

## APPENDIX 1B: TECHNICAL

HEAD OFFICE IT DEPARTMENT

2ND FLOOR,

PLOT NO. 151, SECTOR 44

INSTITUTIONAL AREA, GURUGRAM -122003

| Note | Instruction   |
|------|---|
| 1    | Bidder must mandatorily mention the exact page number & clause or section reference from their submitted technical proposal or OEM product documentation which demonstrate compliance with each criteria (specification). Any Response marked as compliance without a valid page reference/section reference, shall be treated as in-complete and may be liable for rejection/scoring penalties   |
| 2    | Any feature or functionality of the proposed solution that is described in the RFP/FRS as "the solution should support" or "the solution should have the capability" or " Solution should provide" or "Solution should/shall have " shall be deemed to be included in the bidder's proposal and must be made available from Day 1. The Bank shall not bear any additional cost for enabling such features or functionalities, and the bidder shall factor in all such requirements in the Total Cost of the product |
| 3    | All Regulatory guidelines requirements as on the date of Bid Submission should be complied from day 1. Bidder/OEM is also required to comply with all the guidelines (regulatory & statutory) issued during the contract period   |

Primary Storage

In case the model (storage/size/any other spec) is different for different environments, compliance is to be provided for each make/model separately

| Make of the Storage  |  |                         |   |                  |
|----------------------|--|-------------------------|---|------------------|
| Model of the Storage |  |                         |   |                  |
| S.No.                | Minimum Technical Specification  | Vendor Compliance (Y/N) | Reference Page Number/Clause Number in Bidder's Technical documents | Vendor's Remarks |
| 1                    | The proposed array should be an all-NVMe array with active-active multi-controller/node scale-out architecture. The array should be scalable to at-least 4 active-active storage controllers/nodes, Proposed Storage should support non-disruptively upgrades, and proposed <b>storage should support single/Dual drive capacity upgrade</b> .The proposed array should support data in place upgrade to higher models of the same storage family.   |                         |   |                  |
| 2                    | The proposed array should have multi-controller architecture with support of NVMe media for optimal storage performance.   |                         |   |                  |
| 3                    | The proposed array should be an unified storage which support both SAN & NAS   |                         |   |                  |
| 4                    | The proposed array should be configured using all NVMe drives on Industry standard RAID6 and should be able to deliver at least 1,00,000 IOPS (8K block size, 80% Read/20% Write) with sub-millisecond latency for both read & write IOs. Mentioned performance numbers should be achieved with data reduction techniques like Compression & deduplication and data Encryption turned ON. OEM should submit the document / official sizing tool output stating the above-mentioned performance metrics capability of the proposed system. These performance numbers should be delivered after considering the overheads of deduplication, compression and encryption. The capacity to be configured as a single/multiple storage pool which should be accessible to both the controllers simultaneously for Read & Write operations. |                         |   |                  |
| 5                    | Proposed storage solution should be offered with minimum 2 controllers with minimum <b>256GB DRAM Cache memory</b> on the entire storage Solution.<br>The solution should scale to atleast <b>512GB Cache memory</b> by adding additional controller. The proposed array must protect data in cache during a manual power down or an unexpected power outage by vaulting to flash storage.<br>The NVMe SSD capacity drives must not be used for any caching requirements of the storage. The caching requirements of storage must be factored separately   |                         |   |                  |
| 6                    | The proposed array should be designed with full redundancy across all components at both the hardware and software level enabling the system to have 99.9999% availability or more   |                         |   |                  |
| 7                    | The proposed array should support FC, iSCSI, vVols 2.0, NFS v4.0 or above/ SMB 3.1 or above/ FTP / SFTP, NVMe/TCP, NVMe/FC from day one.   |                         |   |                  |
| 8                    | The proposed array should be configured with at least 8 x 32Gbps & 8 x 10Gbps optical front-end ports & Proposed storage should support 100GbE backend.  |                         |   |                  |
| 9                    | The storage must be configured with proposed storage usable capacity after dedupe and compression. It should be scalable to at-least 2x usable flash NVMe capacity on the same storage Array. The storage should support volume movement within the cluster. Addition of controllers/nodes in the same cluster should not cause any downtime and the system should automatically detect and add new controllers/nodes to the cluster.  |                         |   |                  |
| 10                   | The proposed array must support the latest industry standard (No proprietary) dual ported NVMe TLC drives. Array should support mixing of drives of various sizes in same storage pool.  |                         |   |                  |
| 11                   | The proposed array should support enterprise class data services including - Thin Provisioning, Inline Compression & Deduplication, replication. Data reduction must be supported on block and vVol. The data reduction feature should have no performance impact on the storage due to DRR.   |                         |   |                  |
| 12                   | Proposed storage array should support major Operating systems including Windows 2019, 2022, RedHat, SUSE, Ubuntu, Oracle, VMWare etc.  |                         |   |                  |
| 13                   | The proposed array must have capability to create snapshots in the proposed storage array for block, Proposed storage solution should support snapshot creation using ROW/WORM algorithm. Storage arrays should have ability to use snapshot as writable volume. These snapshots should be secure and immutable.   |                         |   |                  |



|    |   |  |  |  |
|----|---|--|--|--|
| 14 | Proposed array should include LUN level priority based QoS engine which is easy to manage. Proposed solution should also have functionality so that a volume with a high-performance policy can be configured handle more IOPS than a volume with a medium-performance policy.  |  |  |  |
| 15 | The proposed array should be proposed with native IP ports for remote replication to DR site with appropriate licenses. If separate FCIP routers are required for replication, then the same should be included in the BOM (Min 2 Nos per site). Proposed storage system should be capable of native storage based asynchronous replication .   |  |  |  |
| 16 | The proposed array should be supplied with native Storage management software with Web based GUI capable of generating customized reports, real time monitoring, at least 1 year of historical performance data for analysis and trending, capacity utilization monitoring.   |  |  |  |
| 17 | Proposed solution should also have cloud-based monitoring and management tool with support for at least 1 year of historical reporting. Software should support monitoring and reporting multiple storage system. Cloud based software is preferably to be accessible from any internet connected device with mobile application support. It should support performance impacts analysis to identify any increases in latency against other metrics such as IOPS and bandwidth.   |  |  |  |
| 18 | The proposed storage solution should support or integrate with software (either OEM-provided or third-party) capable of automating and orchestrating application/database-consistent copies for applications including, but not limited to, MSSQL, Oracle, Exchange, to support use cases such as data repurposing, off-host backup, Test/Dev, Reporting, etc.  |  |  |  |
| 19 | Proposed storage solution should support below integration options to enable DevOps and Infrastructure automation. All mentioned options should be officially supported by storage OEM.<br>a) Support for REST API<br>b) Support for Kubernetes Persistent Volumes using Container Storage Integration (CSI)<br>c) Support for Ansible<br>d) Support for PowerShell modules   |  |  |  |
| 20 | The proposed array must include SED (or hardware) based data at rest encryption solution to encrypt data on all drives (AES 256 bit) with embedded automated key management. Encryption should seamlessly work with all the storage features and without any performance penalty.   |  |  |  |
| 21 | Bank will not return the defective disk(s) in case of disk failure  |  |  |  |
| 22 | On-Cloud: For solutions proposed on the cloud, the bidder must adequately size the primary storage at both the primary and secondary cloud sites based on the requirements of the respective solution(s).<br><br>On-Premises: For solutions proposed on-premises, the bidder must adequately size the primary storage at both the Data Centre (DC) and Disaster Recovery (DR) sites, in line with the needs of the proposed solution(s).<br><br>While proposing Bidder & OEM to right size the storage sizing at both cloud and premise |  |  |  |
|    | <b>EXPERIENCE</b>   |  |  |  |
| 23 | The proposed make of the storage should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI  |  |  |  |

x86 Servers

In case the model (Server/processor/memory/HDD/any other spec) is different for different application/deployment zone/environments, compliance is to be provided for each make/model separately

Make of the server

Model of the server

| S.No. | Item             | Minimum Technical Specification   | Vendor Compliance (Yes/No) | Reference Page Number/Clause Number in Bidder's Technical documents | Vendor's Remarks                     |
|-------|------------------|---|----------------------------|---|--------------------------------------|
| 1     | Processors       | Latest dual processor model (Intel Xeon or AMD EPYC) with base clock speed of 2.8 GHz or better as per the requirement and proposition proposed by the bidder   |                            |   | Provide the proposed processor Model |
| 2     | Chipset          | Processor OEM Chipset compatible with the offered processors.   |                            |   |                                      |
| 3     | Internal Storage | The server should Support minimum 8 hot-swappable SAS,SATA and SSD drives or more   |                            |   |                                      |
| 4     |                  | Server should be supplied with 2x 1.92TB SATA SSD or higher. Bank will not return the defective disk(s) in case of disk failure   |                            |   |                                      |
| 5     |                  | The Server hardware RAID controller should support the following configurations RAID 0, 1, 5, 6, 10, 50, and 60. The raid controller should have minimum 8GB NV cache, capable of supporting minimum 22.5Gb/s SAS or higher   |                            |   |                                      |
| 6     | Memory           | Should be configured with 512GB memory  |                            |   |                                      |
| 7     |                  | Should have minimum 24 number of DIMM slots per server and support 5600MT/s or higher Dual Rank DDR5 memory or higher   |                            |   |                                      |
| 8     | Network          | Support for RAS features like Demand Scrubbing, Patrol Scrubbing & Permanent Fault Detection  |                            |   |                                      |
| 9     | SAN Connectivity | 4x 10G SFP+ Ports with optics   |                            |   |                                      |
| 10    | PCIe Slots       | 2 x Dual Port 32 Gbps FC Card   |                            |   |                                      |
| 11    | Security         | Should have minimum 4 or more PCIe Generation 4.0 slots or higher   |                            |   |                                      |
| 12    |                  | Should have a cyber-resilient architecture for a hardened server design for protection, detection & recovery from cyber attacks   |                            |   |                                      |
| 13    |                  | Should provide effective protection, reliable detection & rapid recovery using:   |                            |   |                                      |
| 14    |                  | Silicon-based Immutable Hardware Root of Trust  |                            |   |                                      |
| 15    |                  | Signed cryptographic firmware updates   |                            |   |                                      |
| 16    |                  | Dynamic USB Port Management   |                            |   |                                      |
| 17    |                  | Secure default passwords  |                            |   |                                      |
| 18    |                  | Shall provide dynamic system lock down server to prevent malicious attacks against embedded firmware and configuration drift in your datacenter without need to reboot the server.  |                            |   |                                      |
| 19    |                  | Persistent event logging including user activity  |                            |   |                                      |
| 20    |                  | Secure alerting   |                            |   |                                      |
| 21    |                  | Should be able to verify BIOS integrity and authenticity from malicious firmware and support automatic BIOS recovery if BIOS is corrupted (either due to a malicious attack, or due to a power loss during the update process, or due to any other unforeseen event).           |                            |   |                                      |
| 22    |                  | Shall support boot from SAN and Rapid OS Recovery In the event of a corrupted OS image  |                            |   |                                      |
| 23    |                  | Support Secure System Erase to erase sensitive data and settings from the server storage devices and server non-volatile stores such as caches and logs so that no confidential information unintentionally leaks   |                            |   |                                      |
| 24    |                  | Configuration upgrades should be only with cryptographically signed firmware and software   |                            |   |                                      |
| 25    |                  | Should provide system lockdown feature to prevent change (or "drift") in system firmware image(s) & prevent malicious modification of server firmware   |                            |   |                                      |
| 26    | Management       | Intrusion alert in case chassis cover being opened  |                            |   |                                      |
| 27    |                  | Real-time power meter, temperature monitoring, customized exhaust temperature and System Airflow Consumption  |                            |   |                                      |
| 28    |                  | Silicon root of trust, authenticated BIOS, signed firmware updates and BIOS Live Scanning for malicious firmware  |                            |   |                                      |
| 29    |                  | Telemetry Streaming   |                            |   |                                      |
| 30    |                  | Idle Server Detection   |                            |   |                                      |
| 31    |                  | Power control, Boot control   |                            |   |                                      |
| 32    |                  | The management software should collect system information (including impending component failure) from the device that generated the alert and should be able to send the information securely to OEM to Support to troubleshoot the issue and provide an appropriate solution. |                            |   |                                      |
| 33    |                  | Support to troubleshoot the issue and provide an appropriate solution.  |                            |   |                                      |
| 34    |                  | OEM's management software should be provided  |                            |   |                                      |
| 35    |                  | Firmware and configuration baselines for compliance monitoring and enable automated updates on schedule.  |                            |   |                                      |
| 36    |                  | Scope based access control to limit Users to specific group of devices  |                            |   |                                      |
| 37    |                  | Bare-metal server deployment and cloning  |                            |   |                                      |
| 38    | Ports            | Should have the following ports for server connectivity   |                            |   |                                      |
| 39    |                  | ● 1 serial port   |                            |   |                                      |

|    |                   |  |  |  |  |
|----|-------------------|--|--|--|--|
| 38 | Others            | ● 3 USB 2.0 ports or higher  |  |  |  |
| 39 |                   | ● 2 VGA port   |  |  |  |
| 40 |                   | Supports hot swappable redundant fans  |  |  |  |
| 41 |                   | Supports hot swappable redundant power supplies  |  |  |  |
| 42 |                   | Sliding Rail Kit to be provided along with the server  |  |  |  |
|    | <b>EXPERIENCE</b> |  |  |  |  |
| 43 |                   | The proposed server make should have been successfully implemented in at least two BFSI clients, each with a minimum of 1,500 branches or offices" |  |  |  |

**Object Storage**

**In case the model (storage/size/any other spec) is different for different environments, compliance is to be provided for each make/model separately**

| Make of the Storage  |  |                         |   |                  |
|----------------------|--|-------------------------|---|------------------|
| Model of the Storage |  |                         |   |                  |
| S.No.                | Minimum Technical Specification  | Vendor Compliance (Y/N) | Reference Page Number/Clause Number in Bidder's Technical documents | Vendor's Remarks |
| 1                    | Storage should be configured with no data loss or data unavailability in the case of both scenarios (a) 4 simultaneous disk failures or (b) 1 node failure. A node is defined as the unit of object storage responsible for storing user data (or a portion of it) on itself and erasure coding it.  |                         |   |                  |
| 2                    | Object Storage shall scale by dynamically adding additional nodes to system, at the granularity of a single node. The upgrades should be carried out non-disruptively online with support for automated data rebalance across the nodes. It should support. Added capacity shall be immediately available in advance of any internal rebalancing of existing data.   |                         |   |                  |
| 3                    | Nodes of different generations (e.g. different processors and disk configurations) must be supported in same object storage system.  |                         |   |                  |
| 4                    | Object storage system must support a multi-site active-active architecture where data can span across multiple geographic locations and provide a global namespace with anywhere read and write access. Storage should be able to provide multisite failure tolerance support to enable seamless operation even though two sites are down  |                         |   |                  |
| 5                    | Object storage must offer functionality to copy locally stored S3 object data to an external S3 target   |                         |   |                  |
| 6                    | All nodes of the object storage system must process write requests and write to different sets of disks to take advantage of all spindles and NICs in cluster.   |                         |   |                  |
| 7                    | Object Storage shall support protocols like S3, S3a, Swift and must support multi-access, allowing same data to be accessed simultaneously. Access to the Object Storage should not be limited to a single writer at a time  |                         |   |                  |
| 8                    | Object storage system should support Active Directory/LDAP integration and should support OpenStack Keystone identity services when utilizing the OpenStack Swift API  |                         |   |                  |
| 9                    | Object storage should support IAM (Identity and access management) with object tagging to enable granular access to resources  |                         |   |                  |
| 10                   | Object Storage shall have ability to set default retention periods for different categories of objects/content in case application(s) cannot specify retention period. Should also support object lock   |                         |   |                  |
| 11                   | Object storage shall allow users to specify expiration policies so that data is automatically removed from the system after defined interval without additional user or application interaction.   |                         |   |                  |
| 12                   | Object Storage shall allow a set retention period when object is first archived and then a specific retention period when triggered by known event (e.g. set retention period of image for X years after an image has been approved for storage).  |                         |   |                  |
| 13                   | Object Storage shall allow hold to be set on a specific object to prevent deletion until hold is released even if it exceeds the object's retention period.  |                         |   |                  |
| 14                   | Object Storage shall protect all objects with Erasure Coding without the dependencies of RAID storage. And the erasure coded data should be encoded equally efficiently, regardless of object size. Object metadata should be stored as 2 or more copies, so operations are not hampered due to any rebuild operation on metadata  |                         |   |                  |
| 15                   | Object Storage shall be WAN optimized by protecting data from local failures using Erasure Coding and from site failures using replication. Object Storage shall support multiple sites (greater than 2).  |                         |   |                  |
| 16                   | Object Storage shall allow any object to be accessed from any node at any site with most recent version of data always available (strong consistency) to the requestor   |                         |   |                  |
| 17                   | Object Storage shall support metadata indexing and search, with ability to apply unlimited metadata tags to the object   |                         |   |                  |
| 18                   | Object Storage must recover from any disk or node failure without connectivity dependency to remote sites.<br>a. All disk and node rebuilds should leverage protection from within the same site so as to avoid consuming expensive and limited WAN bandwidth and minimize rebuild times during rebuild operations.<br>b. On disk or node failure, Object Storage shall redistribute exposed data across as many drives and nodes as possible to take advantage of multiple spindles and minimize data exposure. |                         |   |                  |
| 19                   | Object Storage shall support encryption of all object data, at rest and in-flight.   |                         |   |                  |
| 20                   | Object Storage shall provide versioning capability to protect and record Object-level changes. Should also offer the capability to create multiple copies of objects natively.   |                         |   |                  |

|    |  |  |  |  |
|----|--|--|--|--|
| 21 | To provide heightened security, Object Storage should allow administrators to disable access to the underlying OS without impacting administrative and end-user APIs and functions. It should also allow lockdown of ports not in use to ensure greater security   |  |  |  |
| 22 | Object Storage shall be managed and monitored via integrated UI, CLI & RESTful APIs.   |  |  |  |
| 23 | Object Storage shall support multi-tenant architecture including ability to apply quota limits on specific sections within the object store.   |  |  |  |
| 24 | Object Storage shall support metering capabilities including reporting on capacity, object count, and bandwidth.   |  |  |  |
| 25 | Object Storage should also provide for REST API for more advanced monitoring and auditing capabilities.  |  |  |  |
| 26 | Object storage system should support audit trails through the management GUI   |  |  |  |
| 27 | Object Storage shall support SNMP and Syslog protocols to provide information related to object storage.   |  |  |  |
| 28 | Object storage must support Storage-as-a-Service tenants, detailed metering, self-service portal, multi-tenancy and consumption intelligence.  |  |  |  |
| 29 | Offered object storage should be a hardware appliance in which all hardware and software is offered and supported by a single OEM.   |  |  |  |
| 30 | <p>Bidder &amp; OEM to right size the storage sizing at both cloud and on-premises based on the data ingestion and data retention period defined in the RFP for the respective solutions.</p> <p><b>On-Cloud:</b><br/>For solutions proposed on the cloud, the bidder must adequately size the Object storage at both the primary and secondary cloud sites based on the requirements of the respective solution(s) and retention period defined for the respective solution.<br/>The bidder must ensure that all data, information, and logs—both raw and parsed—are daily transferred to the on-premises object storage infrastructure and should be stored on on-premises object storage for the period of 3 months.</p> <p><b>On-Premises:</b><br/>For solutions proposed on-premises, the bidder must adequately size the Object storage at both the Data Centre (DC) and Disaster Recovery (DR) sites, in line with the needs of the proposed solution(s) and retention period defined for the respective solution</p> |  |  |  |
|    | <b>EXPERIENCE</b>  |  |  |  |
| 31 | The proposed make of the storage should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI   |  |  |  |

**SAN Switch**

**In case the model (Switch/Port Count/Port speed) is different for different environments, compliance is to be provided for each make/model separately**

| <b>Make of the SAN Switch</b>  |   |                                |  |                         |
|--------------------------------|---|--------------------------------|--|-------------------------|
| <b>Model of the SAN Switch</b> |   |                                |  |                         |
| <b>S.No.</b>                   | <b>Minimum Technical Specification</b>  | <b>Vendor Compliance (Y/N)</b> | <b>Reference Page Number/Clause Number in Bidder's Technical documents</b> | <b>Vendor's Remarks</b> |
| 1                              | The switch should have non-blocking architecture with all ports active with 32 G SFP+ modules , switch should also support 64G transceiver for future upgrades.   |                                |  |                         |
| 2                              | The switch should be configured with base 24 port (minimum) and can be upgraded to 48 ports with port-on - demand licenses activation   |                                |  |                         |
| 3                              | The switch should support auto-sensing 64,32,16, 8 Gbit/sec FC capabilities.  |                                |  |                         |
| 4                              | The switch shall support different port types such as D_Port (ClearLink Diagnostic Port), E_Port, EX_Port, F_Port, optional port-type control Brocade Access Gateway mode: F_Port and NPIV-enabled N_Port   |                                |  |                         |
| 5                              | The switch must provide a maximum Aggregate bandwidth of 4Tbps (data rate) end to end or more   |                                |  |                         |
| 6                              | Non disruptive Microcode/ firmware Upgrades and hot code activation.  |                                |  |                         |
| 7                              | The Switch must provide autonomous Congestion control mechanisms without user intervention  |                                |  |                         |
| 8                              | The Switch must be able to automatically quarantine and unquarantine slow-devices   |                                |  |                         |
| 9                              | The Switch must provide Virtual Machine (VMID) support for end-to-end SAN telemetry   |                                |  |                         |
| 10                             | The switch should support Frame-based trunking with up to eight SFP+ ports per ISL trunk; up to 512Gb/s per ISL trunk   |                                |  |                         |
| 11                             | The Switch must support POST and online/offline diagnostics, including RASrtrace logging, environmental monitoring, non-disruptive daemon restart, FCping and Pathinfo (FC traceroute), port mirroring (SPAN port).   |                                |  |                         |
| 12                             | The Switch must support web based management and also support CLI.  |                                |  |                         |
| 13                             | The switch must support 24K frame buffers   |                                |  |                         |
| 14                             | The Switch must support SAN Analytics with parallel SCSI and NVMe-FC analytics  |                                |  |                         |
| 15                             | Should provide redundant and hot pluggable components.  |                                |  |                         |
| 16                             | The switch should support Front to back and back to Front airflow   |                                |  |                         |
| 17                             | The switch should be 1U form factor and rack mountable in a standard Rack   |                                |  |                         |
| <b>EXPERIENCE</b>              |   |                                |  |                         |
| 18                             | The proposed make of the SAN Switch should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI |                                |  |                         |

| Backup Solution/Appliance   |  |                      |   |         |
|---|--|----------------------|---|---------|
| In case the model (Switch/Port Count/Port speed) is different for different environments, compliance is to be provided for each make/model separately |  |                      |   |         |
| Make of the Backup Solution & Appliance   |  |                      |   |         |
| Model of the Backup Solution & Appliance  |  |                      |   |         |
| S.No.   | Minimum Technical Specification  | Compliance ( Yes/No) | Reference Page Number/Clause Number in Bidder's Technical documents | Remarks |
| 1   | Proposed backup Solution will support backup, recovery, Long term archival and restoation from single GUI/ console.  |                      |   |         |
| 2   | Proposed Disk Based Storage/Appliance should be able to interface with various industry leading server platforms, operating systems and Must support LAN/SAN based D2D backup and VTL backup simultaneously via NFS v3/v4, CIFS, FC etc.   |                      |   |         |
| 3   | Proposed Disk Based Appliance/backup storage must support global/in-line data duplication using variable block length de-duplication technology.   |                      |   |         |
| 4   | Proposed Disk Based Appliance/backup storage should be offered with protocols like VTL, CIFS and NFS v3 / v4. All of the protocols should be available to use concurrently   |                      |   |         |
| 5   | Proposed Disk Based Appliance/backup storage should support industry leading backup software like Networker, Dell PPDm Netbackup, Commvault and Data Protector etc and should Support deduplication at backup server/ host / application level so that only changed blocks travel through network to backup device.  |                      |   |         |
| 6   | Proposed Disk Based Appliance/backup storage should have the capability to tier backup data in deduplicated format to an external cloud storage (on premise / public cloud).<br>Proposed backup solution with storage/appliance should have redundant components (Backup Backup Storage - controllers, Power , fans etc. and Backup Appliance - Power , fans etc.) , HA mechanism in place to avoid Single Point of Failure and should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. Proposed Backup Solution should have scalability with respect capacity in future.   |                      |   |         |
| 7   | Proposed Disk Based Appliance/backup storage should have the ability to perform different backup, restore, replication jobs simultaneously and Must supports communications and data transfers through 32 GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The proposed backup appliance should be offered with min. 4 x 10/25 Gbps NIC SFP+, and 2 x 32 Gbps FC ports.<br>or<br>Proposed Disk Based Appliance/backup storage should have the ability to perform different backup, restore, replication jobs simultaneously and Must supports communications and data transfers through 32 GB SAN, 10 Gb & 1 Gb ethernet LAN over copper and SFP+. The Proposed Backup Storage should have should have minimum of 4x16/32 GB FC ports & 2x32G ports on each controller for Host connectivity. |                      |   |         |
| 8   | Proposed Disk Based Appliance/backup storage should support backup throughput of minium 30 TB/hr while maintaining a single deduplication pool with RAID 6 or equivalent and min. one hot spare disk with base and every expansion shelf as well.  |                      |   |         |
| 9   | Proposed Appliance/Backup Storage should support different retentions for primary and DR backup storage and should support instant copy creation on remote site for better DR readiness with support for transmitting only deduplicated unique data in encrypted format to remote sites.   |                      |   |         |
| 10  | The proposed backup Solution must support retention lock or equivalent feature which ensures that no data is deleted accidentally.   |                      |   |         |
| 11  | Backup software/solution should be able to protect the databases (online) through online agents enabling granular restores. Backup Major DBs like Oracle, DB2, MS SQL, Hadoop, MongoDB, Cassandra etc. and Applications etc. across wide range of popular Windows / Linux and Unix flavours  |                      |   |         |
| 12  | Proposed Appliance/Backup Storage should support bi-directional, many-to-one, one-to-many, and one-to-one replication.   |                      |   |         |
| 13  | Proposed Appliance/Backup Storage should support 256 bit AES encryption for data at rest and data in-flight during replication. It should offer internal and external key management for encryption.   |                      |   |         |
| 14  | Proposed Disk Based Storage/Appliance should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user. The disk based backup solution must support global/in-line data duplication.   |                      |   |         |

|    |   |  |  |  |
|----|---|--|--|--|
| 15 | Proposed Disk Based Storage/Appliance should be offered with Multi-Tenancy features which provides a separate logical space for each tenant user. The disk based backup solution must support global/in-line data duplication.  |  |  |  |
| 16 | The Proposed Appliance/Backup Storage must provide verification of the Metadata and actual data of the file with strong Checksum Mechanism  |  |  |  |
| 17 | All file system data and Metadata must be verified continuously even if parts of the file system are never accessed for reads (Automated Data Scrubbing Process)  |  |  |  |
| 18 | Any modification or new data must not modify existing data blocks to prevent possibility of corruption. Any new or modified content must be written to new blocks   |  |  |  |
| 19 | The appliance should be configured with all the licenses backup and replication necessary for the above functionalities   |  |  |  |
| 20 | The Proposed Appliance/Backup Storage must provide mechanism to restrict any date and time change of the system to protect against any accidental or intentional expiration of data through change in the Network Time internally or externally to the system   |  |  |  |
| 21 | Proposed Appliance/Backup Storage must offer with feasibility to protect data from accidental deletion  |  |  |  |
| 22 | Regular Maintenance activities like Systems Housekeeping/Garbage Cleaning etc should be able to happen simultaneously along with regular backup and restore operations without having the need for a dedicated window   |  |  |  |
| 23 | Should be able to integrate with native backup interfaces of Hyper Converged Solutions in future agentless and/or image level backup of VMs   |  |  |  |
| 24 | Should be able to protect data by backing it up to another disk target with different hardware or tape target. All necessary licenses for achieving the functionality should be provided  |  |  |  |
| 25 | Product should offered with 24x7- 5 years(Contract period, whichever is later) onsite warranty support.   |  |  |  |
| 26 | The backup should provide Data protection, Ransomware protection & Scan, and Ransomware security review/ Dashboard & for this licenses should be provided from day1.  |  |  |  |
| 27 | The Proposed solution should ensure Data Protection & Archival:<br>a) Backup and Recovery: Protects data by creating secure backups and enables fast recovery in case of failures or cyber incidents.<br>b) Data Immutability & Encryption: Ensures that sensitive data is protected both in transit and at rest using strong encryption methods.<br>c) Data Integrity and Availability: Ensures that data remains intact and available for recovery in case of an outage, system failure, or cyberattack.<br>d) Archival: Reduces the cost of storing inactive or less frequently accessed data.<br>e) Compliance and Legal Hold: Ensures that data is retained for the necessary period as required by regulatory bodies and the organization's internal policies.<br>f) Search and Retrieval: Enables fast and efficient retrieval of archived data, ensuring that critical information can be accessed quickly when needed.<br>g) Long Term Retention/Forever Retention: Covers a "No Loss of Data" policy using long-term retention. |  |  |  |
| 28 | The proposed backup software should be independent of storage hardware  |  |  |  |
| 29 | The Backup software must be able to compress and encrypt data and should also support de-duplication.   |  |  |  |
| 30 | Proposed solution with appliance must support immutability or WORM (Write Once Read Many) or Data Retention lock feature for storing backups  |  |  |  |
| 31 | Offered solution should support writing the long term retention copies of the backup data on Long term Storage and required software licenses for the Long term retention on Long term Storage  |  |  |  |
| 32 | Solution should provide historic backup & retrieval reports for success & failure Daily, Monthly & Quarterly or as per Bank requirement.  |  |  |  |
| 33 | The solution should provide data validation features to ensure data integrity by validating data integrity during backup, when data is at rest and during data copy operations.   |  |  |  |
| 34 | The proposed backup & retrieval solution should ensures all data, logs, and information related to the respective solutions proposed under this RFP—regardless of whether the solution(s) are deployed on-cloud or on-premises.   |  |  |  |



|    |  |  |  |  |
|----|--|--|--|--|
| 35 | <p>The following backup and retention policy to ensure data protection, recoverability, and compliance with long-term retention needs is complied:</p> <ul style="list-style-type: none"> <li>• Daily Incremental Backup – retained for 2 weeks in disk-based appliance/backup storage</li> <li>• Weekly Full Backup for all data types – Retained for 6 weeks in disk-based appliance/backup storage</li> <li>• Monthly Full Backups – Retained for 4 Months in the same appliance/backup storage</li> <li>• Quarterly Full Backups* - Retained for 6 months in the same appliance//backup storage.</li> </ul> <p>*After the 6-month period, Quarterly Full backups must be migrated to long-term backup storage, where they shall be retained for the entire duration of the contract.</p> <p>Backup Appliance / Backup Storage Requirements</p> <p>* Online Backup Storage/Appliance must retain backups for a minimum period of 6 months, with each quarterly backup being preserved during this duration.</p> <p>* All quarterly backups taken during the contract period must also be stored on long-term (offline) storage for the entire duration of the contract.</p> <p>*All the data, logs, information &amp; others must be backed up using the proposed backup and retrieval solution, in accordance with the defined backup policy and retention requirements.</p> <p>*Regularly test and verify the integrity of backed-up data and information by performing retrieval exercises. This process should be completed prior to overwriting or replacing any previously taken backups, to ensure that the data is recoverable, intact, and usable when required.</p> |  |  |  |
| 36 | Backup is to be performed at both DC and DR. The Proposed solution must have Disk to Disk to Long term Storage (D-D-LTS) Backup solution with backup data to be kept on disk for easy retrieval.   |  |  |  |
| 37 | Backup & retrieval Solution, Backup Storage/Appliance is to be proposed at both DC & DR with all requisite licenses.   |  |  |  |
|    | <b>EXPERIENCE</b>  |  |  |  |
| 38 | The proposed make and category of the backup solution & appliance should have been implemented in at least 2 scheduled commercial bank with 1500 branches for security solutions/Core banking system/ Datawarehouse/Datalake/Other critical system of the bank like treasury/NEFT RTGS/BFSI  |  |  |  |

Long Term Storage

In case the model is different for different environments, compliance is to be provided for each make/model separately

| Make of the Long Term Storage |   |                     |   |         |
|-------------------------------|---|---------------------|---|---------|
| Model of Long Term Storage    |   |                     |   |         |
| S.No.                         | Minimum Technical Specification   | Compliance (Yes/No) | Reference Page Number/Clause Number in Bidder's Technical documents | Remarks |
| 1                             | Proposed storage would be proposed for long retention of Backup data (Protocol- NAS/CIFS/SMB/S3/SAN storage (Protocol- iSCSI))  |                     |   |         |
| 2                             | Bank is looking for Long term storage for the duration of the Contract. Bidder to design and propose the solution for storing the backups for the duration of the contract with adequate interfaces for performing the backup & retrieval within the defined period and as per the terms of the RFP.<br>Interface should be design to ensure that Data / logs/Informations are in the proposed storage after the duration mentioned in the RFP.<br>The Backed up data / logs need to be restored in the respective technology for forensic and other requirement of the bank etc. |                     |   |         |
| 3                             | Bank is looking for Long term storage for the duration of the Contract. Bidder to design and propose the solution for storing the backups for the duration of the contract with adequate RAID.<br>Proposed Sizing should be proposed on RAID 6  |                     |   |         |
| 4                             | <ul style="list-style-type: none"> <li>Bidder is required to propose the long-term backup storage at both the Data Centre (DC) and Disaster Recovery (DR) sites and must adequately sized the storage to retain backup data for the entire duration of the contract.</li> <li>The sizing should account for data growth, retention policies, and restore requirements, ensuring reliable and compliant backup management throughout the contract period.</li> </ul>   |                     |   |         |
| <b>EXPERIENCE</b>             |   |                     |   |         |
| 5                             | The proposed make and category of the storage should have been implemented in at least 2 scheduled commercial bank with 1500 branches   |                     |   |         |

Load Balancer

In case the model is different for different environments, compliance is to be provided for each make/model separately

|                            |  |  |  |
|----------------------------|--|--|--|
| Make of the Load Balancer  |  |  |  |
| Model of the Load Balancer |  |  |  |

| S.No. | Minimum Technical Specification   | Compliance ( Yes/No) | Reference Page Number/Clause Number in Bidder's Technical documents | Remarks |
|-------|---|----------------------|---|---------|
| 1     | The proposed solution should be a dedicated appliance as ADC not as add on license Feature on NGFW and WAF.   |                      |   |         |
| 2     | The Appliance should have dedicated 1x1GbE port for management and 6x10GbE SFP+ ports and multicore CPU, minimum 4 TB HDD and dual power supply.  |                      |   |         |
| 3     | The SLB OEM should be different from Web Application Firewall OEM and support 7K SSL TPS for RSA 2K key, 10K SSL TPS for ECDSA P25  |                      |   |         |
| 4     | The appliance should have dedicated SSL Acceleration hardware card for handling SSL Traffic. The SSL traffic should not be process by CPU of the appliance  |                      |   |         |
| 5     | The solution should able to load balancer both TCP and UDP based applications with layer 2 to layer 7 load balancing including WebSocket and WebSocket Secure.  |                      |   |         |
| 6     | The solution should support server load balancing algorithms i.e. round robin, weighted round robin, least connection, Persistent IP, Hash IP, Hash Cookie, consistent hash IP, shortest response, proximity, SNMP, SIP session ID, hash header etc.                          |                      |   |         |
| 7     | The solution should support Multi-level virtual service policy routing , -Static, default and backup policies for intelligent traffic distribution to backend servers   |                      |   |         |
| 8     | The solution should support for policy nesting at layer 7 and layer 4. it should able to combine layer4 and layer7 policies to address the complex application integration.   |                      |   |         |
| 9     | The solution should have script based functions support for content inspection, traffic matching and monitoring of HTTP, SOAP, XML, diameter, generic TCP, TCPS. It should support ePolicies to customize new features/rules to re-direct the traffic on specific parameters. |                      |   |         |
| 10    | The solution using e-policy then should support algorithms including round robin, least connections, shortest response, persistence ip, hash ip, hash ip and port, consistent hash IP and snmp  |                      |   |         |
| 11    | The solution should provide application & server health checks for well-known protocols such as ARP, ICMP, TCP, DNS, RADIUS, HTTP/HTTPS, RTSP etc.  |                      |   |         |
| 12    | The Solution should provide real time Dynamic Web Content Compression to reduce server load and solution should provide selective compression for Text, HTML, XML, DOC, Java Scripts, CSS, PDF, PPT, and XLS Mime types.  |                      |   |         |
| 13    | The solution should provide advanced high performance memory/packet based reverse proxy Web cache; fully compliant with HTTP1.1 to enhance the speed and performance of web servers   |                      |   |         |
| 14    | The solution should provide support for cache rules/filters to define granular cache policies based on cache-control headers, host name, file type, max object size, TTL objects etc..  |                      |   |         |

|    |  |  |  |  |
|----|--|--|--|--|
| 15 | The proposed load balancing solution should support a license upgrade mechanism that allows for the enablement of additional features on the same physical or virtual appliance, without requiring hardware replacement. Where applicable, the solution should be capable of integrating with or supporting secure machine-based authentication mechanisms for access to <del>the solution</del> |  |  |  |
| 16 | The solution should provide secure online application delivery using hardware-based high performance integrated SSL acceleration hardware. SSL hardware should support both 2048,4096 bit keys for encrypted application access.   |  |  |  |
| 17 | The solution must support Single Sign-On (SSO) for web based applications and web based file server access. It should also supports SAML secure application access   |  |  |  |
| 18 | The solution should provide performance optimization using TCP connection multiplexing, TCP buffering and IEEE 802.3ad link aggregation. Support for TCP optimization options including windows scaling, timestamp & Selective Acknowledgement for enhanced TCP transmission speed TCP optimization option configuration should be defined on per virtual service basis not globally.            |  |  |  |
| 19 | The solution should support certificate parser and solution should integrate with client certificates to maintain end to end security and non-repudiation. It should support Certificate format as "OpenSSL/Apache, *.PEM", "MS IIS, *.PFX", and "Netscape, *.DB".   |  |  |  |
| 20 | The solution should support OCSP protocol to check the validity of the certificates online. Certificate bases access control, CRL's (HTTP, FTP, and LDAP) support.   |  |  |  |
| 21 | The solution should provide full ipv6 support and OEM should be IPv6 gold-certified. OEM should be listed vendor for ipv6 phase-2 certification.   |  |  |  |
| 22 | The solution should support advance ACL's to protect against network based flooding attacks. Administrator should able to define ACL's rules based on connections per second (CPS) and concurrent connections (CC), cookie value.  |  |  |  |
| 23 | Should support QOS for traffic prioritization, CBQ , borrow and unborrow bandwidth from queues. It should provide QOS filters based on port and protocols including TCP, UDP and ICMP Protocols. Should support rate shaping for setting user defined rate limits on critical application.   |  |  |  |
| 24 | The solution should support site selection feature to provide global load balancing features for disaster recovery and site redundancy.  |  |  |  |
| 25 | It should support advance functions Authoritative name sever, DNS proxy/DNS NAT, full DNS server with DNSEC, DNS DDOS, application load balancing from day one. It should be capable of handling complete Full DNS bind records including A,MX, AAAA, CNAME, PTR, SOA etc.   |  |  |  |
| 26 | The solution should provide comprehensive and reliable support for high availability and N+1 clustering based standard VRRP RFC 2338 on Per VIP based Active-active & active standby unit redundancy mode.   |  |  |  |
| 27 | the solution should support Stateful session failover with N+1 clustering support when deployed in HA mode. The solution should support USB based FFO cable to synchronize configuration at boot time of HA  |  |  |  |
| 28 | The solution should support floating MAC address to avoid MAC table updates on the upstream routers/switches and to speedup the failover. It should support for secondary communication link for backup purpose  |  |  |  |
| 29 | The solution should support floating IP address and group for stateful failover support. Appliance must have support 256 floating ip address for a floating group. It should support built in failover decision/health check conditions including, CPU overheated, system memory, process health check, unit failover, group failover and reboot   |  |  |  |
| 30 | The solution should also have option to define customized rules for gateway health check - the administrator should able to define a rule to inspect the status of the link between the unit and a gateway   |  |  |  |
| 31 | The appliance should have extensive reporting and logging with inbuilt tcpdump like tool and log collection functionality. The appliance should have SSH CLI, Direct Console, SNMP, Single Console per Cluster with inbuilt reporting.   |  |  |  |
| 32 | The solution should support XML-RPC for integration with 3rd party management and monitoring of the devices. The appliance should provide detailed logs and graphs for real time and time based statistics   |  |  |  |

|    |   |  |  |  |
|----|---|--|--|--|
| 33 | The appliance must support multiple configuration files with 2 bootable partitions for better availability and easy upgrade / fallback. The system should support led warning and system log alert for failure of any of the power and CPU issues |  |  |  |
| 34 | OEM should have TAC & R&D facility in INDIA. OEM should be present in India from last 12 Years.   |  |  |  |

| To be provided by CSP provider on their Letterhead |   |                         |   |                  |
|--|---|-------------------------|---|------------------|
| S.No.  | Minimum Technical Specification   | Vendor Compliance (Y/N) | Reference Page Number/Clause Number in Bidder's Technical documents | Vendor's Remarks |
| 1  | Cloud must be hosted in India, and there should be no network and data sharing/replication to any datacenter/office outside the boundaries of India.<br>The CSP will be bound by Indian law, Indian IT Law, and the applicable regulations. No data in any circumstances should be shared/copied/transmitted without' s consent/written permission of the bank and it should be as per the Indian IT Law, RBI guidelines, bank policy & guidelines and other regulatory & statutory body in India |                         |   |                  |
| 2  | Requisite provisioning of network infrastructure (including switches, router, firewalls, and load balancers) to ensure accessibility of the servers as per defined SLA's.<br>All the equipment's/Devices in the path must be in HA mode with no single point of failure.  |                         |   |                  |
| 3  | The proposed cloud infrastructure should be deployed in High Availability mode (N+N) at both primary site and secondary site.<br>Non-production environment should be 10% of production (primary site) environment.   |                         |   |                  |
| 4  | CSP should have a multi-site infrastructure setup, with network performance between them sufficient to accomplish synchronous replication, so that Bank can architect for high availability with defined RTO and RPO.   |                         |   |                  |
| 5  | Data Centers of CSP should be minimum Rated 3 of TIA940 or Tier 3 of Uptime Institute or any other equivalent certification   |                         |   |                  |
| 6  | CSP should be empaneled with the Ministry of Electronics and Information Technology (MeiTY)   |                         |   |                  |
| 7  | The CSP should have experience of provisioning Services on their Cloud for at least 3 clients in India (Private/ PSU/ Central Govt/ State Govt. or any other Organization or agencies) of which 1 should be a PSU/ Central Govt/ State Govt during last 5 years as on the date of bid submission  |                         |   |                  |
| 8  | CSP should perform regular tech refreshes, patch management and other operations of provisioned infrastructure that is in the scope of the CSP under this RFP.  |                         |   |                  |
| 9  | The CSP shall provide bank with the necessary logs for the services for security monitoring and incident alert management.  |                         |   |                  |
| 10   | CSP shall provide interoperability support with regards to available APIs, data portability etc. for to utilize in case of change of bidder, migration back to in-house infrastructure, burst to a different cloud bidder for a short duration or availing backup or DR services from a different bidder.   |                         |   |                  |
| 11   | The CSP should adhere to the relevant standards published (or to be published) by DeitY/MeitY or relevant standards body setup or regulator like RBI, SEBI, AMFI / recognized by Government of India and notified to the bidder or CSP by DeitY/MeitY/SEBI/AMFI/RBI/or by any institution recognized by Govt. of India as a mandatory standard and/or regulations.  |                         |   |                  |
| 12   | Bank will have right to audit the data center facilities of CSP through any regulators or through any third parties as needed by the regulators and this may entail data localization, sovereignty, confidentiality, and such other things. It's bidder responsibility to enable the same, necessary provision should be incorporated by bidder with CSP to ensure the compliance to the same.  |                         |   |                  |
| 13   | The CSP should provide bank the third-party audit reports on information security & data integrity, source code review including APIs, details about APIs encryption of payloads, authorization, and authentication API wise - every year irrespective of any audit on demand.  |                         |   |                  |
| 14   | The CSP shall ensure to protect confidential information from unauthorized disclosure and use   |                         |   |                  |
| 15   | Each of the environments provided should be logically isolated, i.e., separate from the production environment in a different VLAN than the production environment and setup such that users of the environments are in separate networks.  |                         |   |                  |
| 16   | If Indian government demand is received for any data, the process mentioned below has to be followed:   |                         |   |                  |
| 16.1   | Disclosure of data of any kind on legal/statutory compulsion should be done only after obtaining concurrence from the Bank.   |                         |   |                  |
| 16.2   | Resist illicit demands that are invalid which are not permitted by the Indian Government or Indian IT Law or any other Indian Regulatory Authorities.   |                         |   |                  |
| 17   | CSP should have capability to provide Alerts & Monitoring interface. Solution should support Remote Administration for administrators   |                         |   |                  |
| 18   | CSP should have Capability to integrate with the authentication servers (LDAP/ADFS etc.) and Integration with applications using API.   |                         |   |                  |
| 19   | The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone   |                         |   |                  |

|      |   |  |  |  |
|------|---|--|--|--|
| 20   | Any data transmission and storage should be encrypting data both at rest and in transit with SSL/TLS (minimum TLS 1.2).   |  |  |  |
| 21   | The Service uptime agreement for the proposed solution on cloud should have monthly uptime commitments and have transparent monthly credit calculations in case of uptime not being met for any services.   |  |  |  |
| 22   | The same Service Level Agreement should be applicable to all included or related services or components that is required for the solution to be contracted for the requirement.   |  |  |  |
| 23   | The proposed solution should not mandate any minimum number of users for any service uptime calculations.   |  |  |  |
| 24   | The proposed solution should also have Service level commitments for virus detection and blocking, spam effectiveness, false positives as well as email delivery.   |  |  |  |
| 25   | Perform regular backup and recovery tests at cloud primary and secondary sites as well as enable sharing the data, configurations rules and policies with the bank for backup at bank's premise.  |  |  |  |
| 26   | CSP's personnel controls are to be in place to provide a logical segregation of duties.   |  |  |  |
| 27   | Measured Service: Resource usage should be monitored, controlled, and reported; providing transparency for both the Bidder and Bank of the utilized service. Bidder should have reporting mechanism to measure the service/performance/availability level criteria as in SLA while billing or as an when Bank requires.   |  |  |  |
| 28   | Resource pooling / Multi-tenancy: There must be a logical separation between each consumer's computing resources and network using virtualization and VPNs or other techniques in case of multi tenancy public cloud setup. Bidder should provide details on how to segregate and protect Bank's data from other customer data in cloud environment.  |  |  |  |
| 29   | Secure Data Deletion: Require that Bidder offer a mechanism for reliably deleting data on Bank's request ensuring no data reminiscence  |  |  |  |
| 30   | Bidder should provide the design and process for data deletion in the scope of an independent audit and that the operational effectiveness of these controls is tested. The report for the same should be submitted to bank as and when asked by bank.  |  |  |  |
| 31   | Bidder should provide confirmation to the Bank that Bank's data is rendered permanently inaccessible and the same should not remain available in any backup or distributed online media after exit of the contract.   |  |  |  |
| 32   | Bidder should provide right to audit as similar what Bank is having with shared data centers in India. In addition:   |  |  |  |
| 32.1 | a. Bank's data should not cross Indian geographical boundaries (physically or logically).   |  |  |  |
| 32.2 | b. Bank must have "Rights to Audit" the CSP's compliance with the agreement including rights of access to the CSP's premises where relevant records and Bank's data is being held.  |  |  |  |
| 32.3 | c. Audit rights for the Bank or its appointed auditor (nominee) or regulators should be integral clause in agreement.   |  |  |  |
| 32.4 | d. Integration of all devices with Bank's SOC, SIEM & other security solution for monitoring.   |  |  |  |
| 32.5 | e. Bank should have access/ monitoring mechanism for Privilege user access (of CSP) to cloud based systems.   |  |  |  |
| 33   | Virtual environment security: It includes resource allocation, hardening of OS, VM image encryption, VM monitoring, USB disabling on VMs, VM should be kept on dedicated partition and IP addresses should not be shared.   |  |  |  |
| 34   | Encryption and Key Management: Depending on sensitivity data is to be encrypted, transport layer encryption is to be ensured using SSL, VPN Gateway, SSH and TLS encryption. End-to-end process for managing and protecting encryption keys to be established and documented. Compliance is to be ensured on ongoing basis.   |  |  |  |
| 35   | Monitoring: Devices should be integrated with Bank's SOC, if so desired, for continuous monitoring for access monitoring, threat monitoring, audit logging, system usage monitoring, protection of log information, administrator and operator log monitoring, fault log monitoring   |  |  |  |
| 36   | The bidder shall provide the artifacts, security policies and procedures demonstrating its and CSP's compliance with the Security Assessment and Authorization requirements.  |  |  |  |
| 37   | In addition to Cloud Security (which includes protection of cloud data, support regulatory compliance & protect customers' privacy), the information security controls including change management, identity and access management, cryptographic controls, network security, data security, vulnerability management, virtualization security, Business continuity, incident management, log monitoring etc. should be implemented by on Cloud by CSP at all locations |  |  |  |

|      |  |  |  |  |
|------|--|--|--|--|
| 38   | Controls related to Operations Security shall be implemented for ensuring Secure Configuration, Application, OS, DB, Web Server, Back-up & Recovery, Change Management, Capacity & Demand Management, Protection against Malicious Code and Monitoring, Auditing & Logging security requirements and any other as required by bank on cloud.           |  |  |  |
| 39   | Reverse Data Shifting: In the event of completion of the contract in normal course or on termination of contract, bidder shall shift the data back to Bank or any of its designated 3rd party's on-premises/ cloud hosted infrastructure. The bidder should sort out operability issue, if any, for smooth shifting of such data.                      |  |  |  |
| 40   | Bank shall be evaluating the operations of the cloud services subscribed & implemented & effectiveness of security controls in the Cloud Computing environment, bidder should enable bank in monitoring the same by providing requisite access, periodic reports, and management Information & dashboard material for reporting on control assessments |  |  |  |
| 41   | The bidder should ensure Data segregation, confidentiality, privacy controls setup in line with the bank's requirement   |  |  |  |
| 42   | In case of Exit/ change of CSP, bidder to ensure the following while formulating the exit plan   |  |  |  |
| 42.1 | i. Removal of all Bank's data on the cloud and assurance that all data has been rendered irrecoverable, upon termination of the cloud outsourcing arrangement in a time-bound manner.  |  |  |  |
| 42.2 | ii. Bidder shall detail out procedures to be used for deletion/destruction of data in a manner that data is rendered irrecoverable.  |  |  |  |
| 42.3 | iii. Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).  |  |  |  |
| 42.4 | iv. Transferability of cloud outsourced services to a third party, another CSP or on premise to the Bank for continuity of service.  |  |  |  |
| 42.5 | v. The format and manner in which data is to be returned to the Bank, as well as support from the CSP to ensure accessibility of the data.   |  |  |  |
| 43   | Cloud architecture shall account for and shall be submitted by bidder regularly at periodic interval to bank:  |  |  |  |
| 43.1 | a. Type of workload,   |  |  |  |
| 43.2 | b. Requirements of availability and resiliency,  |  |  |  |
| 43.3 | c. Security,   |  |  |  |
| 43.4 | d. Authentication,   |  |  |  |
| 43.5 | e. Performance,  |  |  |  |
| 43.6 | f. Operations and management.  |  |  |  |
| 43.7 | g. Logical segregation   |  |  |  |
| 44   | Security has been implemented at all layers i.e., Physical, Network, Data, Application, etc., of cloud architecture with multiple security controls.   |  |  |  |
| 45   | Bank's data should be isolated from other customers, to avoid comingling of data, in case of multi-tenancy.  |  |  |  |
| 46   | Cloud workload is protected against network-based attacks by implementing controls such as:  |  |  |  |
| 46.1 | a. Network segregation of workloads on the cloud shall be implemented based on their type (production, test, development) and purpose (user, server, interface, critical infrastructure segments etc.).  |  |  |  |
| 46.2 | b. A dedicated security network segment (landing segment) shall be implemented for terminating all ingress traffic to the cloud.   |  |  |  |
| 46.3 | c. All internet traffic to the workload on cloud shall be routed through DMZ. Other network segments in the cloud environment shall not have direct access to the Internet.  |  |  |  |
| 46.4 | d. Micro Segmentation shall be implemented on the cloud.   |  |  |  |
| 46.5 | e. All network segments in the Cloud environment shall be protected with security controls such as Firewall, IPS/IDS, anti-DDoS, AV, DLP, WAF, NAC etc.  |  |  |  |
| 46.6 | f. Direct network connection with cryptographic controls shall be implemented to secure the traffic between the cloud and on-premises environment.   |  |  |  |
| 47   | Implement principle of selective privileges and impose segregation of duties with appropriate access and authorization:  |  |  |  |
| 47.1 | a. To manage access rights to cloud services by the Bank's users, the CSP should provide user access management functions to the Bank.   |  |  |  |
| 47.2 | b. Segregation of privileged users and their activities must be documented. Access Control and Role Conflict Matrix to be defined and implemented. Access to Master/ Admin account for Cloud deployment shall be used by exception and shall not be used for operational activities.   |  |  |  |
| 47.3 | c. Multifactor authentication shall be implemented for user access to critical workloads and for all privileged access on the cloud.   |  |  |  |



|       |   |  |  |  |
|-------|---|--|--|--|
| 47.4  | d. Users with privileged system access shall be clearly defined and regular user access reviews, at least once every three months, shall be conducted.  |  |  |  |
| 47.5  | e. Remote access by administrators and privileged users to the cloud environment over the Internet, shall not be permitted.   |  |  |  |
| 47.6  | f. In case of workloads providing compute resources over the Internet, remote access security measures such as two factor authentication and Virtual Private Network (VPN)/ encryption shall be implemented. Cloud-based virtual machine instances with a public IP shall not have open Remote Desktop Protocol (RDP)/Secure Shell Protocol (SSH) ports. Any system with an open RDP/SSH port shall be placed behind a firewall and require users to use a VPN to access it through the firewall. |  |  |  |
| 47.7  | g. Cloud Service Provider/ Cloud Management Team should not have access to any application data of the Bank.  |  |  |  |
| 47.8  | h. Conditional access should be implemented for privileged users.   |  |  |  |
| 47.9  | i. Legacy authentication protocols should be disabled.  |  |  |  |
| 44.10 | j. A granular access control policy should be implemented for access to any cloud resource.   |  |  |  |
| 48    | To ensure confidentiality, integrity and non-repudiation of data-in-transit and data-at-rest, encryption controls in line with Bank's Cryptographic Policy, shall be implemented to secure data stored/processed/ transmitted in the cloud including data backups and logs.   |  |  |  |
| 48.1  | a. Critical/ sensitive data including PII/ SPDI, card holder data or account numbers shall be masked or encrypted.  |  |  |  |
| 48.2  | b. Bank shall have an option to implement 'Bring Your Own Key' as and when required.  |  |  |  |
| 48.3  | c. In case cloud based HSM is used, it should meet the FIPS 140-2 Level 3 and above criteria.   |  |  |  |
| 48.4  | d. HSMs and other cryptographic material should be stored on segregated secure networks with stringent access controls.   |  |  |  |
| 48.5  | e. In case CSP's keys are being used for encryption of Bank's data, such keys should be unique and not shared by other users of the cloud service.  |  |  |  |
| 49    | Retention of Bank's data on the cloud shall be in accordance with the extant guidelines of Bank's Data Retention Policy.  |  |  |  |
| 50    | Web Application Firewall shall be implemented on the cloud for Web based applications. WAF application signature should be updated and reviewed regularly. The Report shall be submitted to bank on a period interval   |  |  |  |
| 51    | Secure Software Development Lifecycle (Secure SDLC) shall be followed for all applications in the cloud throughout the application lifecycle. Security assurance certificate shall be provided by the bidder to the bank for applications provided by CSP/ Third Party.   |  |  |  |
| 52    | Secure Cloud APIs shall be implemented to develop the interfaces to interact with cloud services. Application integration and information exchange should happen over secured API channels.   |  |  |  |
| 53    | The systems in cloud infrastructure should be periodically updated with the latest anti- malware signatures, the bidder shall submit the period report on the same with bank  |  |  |  |
| 54    | Data Loss Governance and risk management framework shall be defined by bidder for workload on the cloud and same shall be shared with bank on periodic basis. Data loss prevention controls should be implemented to secure the data in the cloud environment from unauthorized or inadvertent exfiltration.  |  |  |  |
| 55    | File integrity monitoring should be implemented in order to ensure authenticated changes and to detect unapproved changes to files.   |  |  |  |
| 56    | Password Policy on the Cloud setup should be minimum as per the Bank's password Policy. For privileged users, it should be more stringent than that for normal users.   |  |  |  |
| 57    | Mechanism shall be implemented to detect service faults or outages in the cloud environment.  |  |  |  |
| 58    | Appropriate Business Continuity Plan and Disaster Recovery Plan shall be put in place for the workload on the cloud, based on the risk assessment. Bidder shall incorporate the business continuity requirements of the Bank in its BCP and DR Plan for Bank's workload. In case of critical workloads, bidder's or CSP's plans should be shared with the Bank  |  |  |  |
| 59    | Change/Configuration management procedures shall be aligned with the Bank's Change Management policy, including change request, approval procedures and notification mechanism.   |  |  |  |
| 60    | The cloud infrastructure should be periodically updated with the latest patches and assurance for the same shall be shared by bidder periodically (once in three months or as per bank's discretion).   |  |  |  |
| 61    | Secure configuration settings related to OS/ database/ network devices/ virtual machines/ middleware should be implemented as per Bank's SCD or equivalent hardening guidelines.  |  |  |  |
| 62    | The cloud environment should follow the Bank's logging and monitoring policy.   |  |  |  |

|      |   |  |  |  |
|------|---|--|--|--|
| 63   | Audit logging should be enabled on all systems on cloud. An audit trail of user access event logs should be maintained to ensure compliance towards regulatory requirements. Duration of retention of Log & data in cloud should be in accordance with extant Data Retention Policy of the Bank.                      |  |  |  |
| 64   | All logs of assets related to Bank's subscription/ tenant should be integrated with the Bank's SOC.   |  |  |  |
| 65   | Bidder shall regularly monitor the use of cloud services, forecast capacity requirements, and accordingly normalize the resources, post approval from bank, to prevent information security incidents caused by resource shortages /malfunctions  |  |  |  |
| 66   | Roll-out / phasing-out of applications to / from cloud should follow the Data Migration Policy of the bank.   |  |  |  |
| 67   | For secure deletion/destruction of data:  |  |  |  |
| 67.1 | a. Do not use CE to purge media if the encryption was enabled after sensitive data was stored on the device without having been sanitized first.  |  |  |  |
| 67.2 | b. Do not use CE if it is unknown whether sensitive data was stored on the device without being sanitized prior to encryption.  |  |  |  |
| 68   | Information Security Awareness (including Bank's policies), education and training programs should include secure best practices for usage of Cloud, Cloud specific risks etc. to relevant stakeholders.  |  |  |  |
| 69   | Evidence of periodic security assessment of cloud environment such as Threat & Vulnerability Risk Assessments or equivalent or independent security assessments, should be provided by bidder at Quarterly intervals and/or as required by bank.  |  |  |  |
| 70   | Periodic Security Assessments shall be performed to identify and mitigate risks in the Cloud setup and evidence for the same should be provided to the bank.  |  |  |  |
| 71   | Bidder should arrange to ensure that periodic Vulnerability Assessment and Penetration Testing (VAPT) on periodic basis is performed on assets provisioned for Bank in cloud infrastructure at Quarterly intervals or as required by bank.  |  |  |  |
| 72   | Comprehensive Security Review (CSR) of the application/service on the cloud shall be conducted on yearly or bi-yearly or as defined by bank basis depending on the type of workload. Information security reviews should be conducted in case of transition or changes of bidder or CSP or during renewal of services |  |  |  |
| 73   | Information security incident management process shall be established to discover, report, respond and prevent information security events and weaknesses effectively by bidder and CSP   |  |  |  |
| 74   | Security incidents should be notified to the relevant stakeholders and escalated in accordance with an escalation matrix and timelines formulated as per the criticality of the workload and in accordance with regulatory and extant guidelines.   |  |  |  |
| 75   | Requirements for forensic investigation including mechanism for acquisition of log data from CSP should be documented and reviewed & approved by bank.  |  |  |  |
| 76   | Bidder shall provide reasonable access to necessary information to assist in any Forensic investigation arising due to an incident in the cloud   |  |  |  |
| 77   | The IS controls' implementation should cover all locations that support Bank's data storage and/ or processing requirements.  |  |  |  |
| 78   | Bidder to regularly and/or as per the frequency defined by bank should submit evidence of conducting DR drills, and lessons learnt and their detailed recordings.   |  |  |  |
| 79   | Default admin and root users should be deleted/disabled, and access should be based on user specific IDs and all such accesses should be logged   |  |  |  |
| 80   | Bidder should deploy Active Directory (AD), Single Sign On (SSO) and strong Password Policy for End point and application access  |  |  |  |
| 81   | Proper access control is to be defined for protecting PSB data and access to the Data is strictly on Need-to-Know Basis   |  |  |  |
| 82   | Log generation, storage and review process should be certified by CERT IN empaneled auditor, report for the same shall be submitted by bidder as and when required by bank  |  |  |  |
| 83   | Bidder confirms and agrees the following:   |  |  |  |
| 83.1 | a. Right to audit to PSB with scope defined.  |  |  |  |
| 83.2 | b. Right to recall data by PSB.   |  |  |  |
| 83.3 | c. System in place of taking approvals for making changes in the application.   |  |  |  |
| 83.4 | d. Regulatory and Statutory compliance at vendor site.  |  |  |  |
| 83.5 | e. IT Act 2000 & its amendments, and other Acts/Regulatory guidelines   |  |  |  |
| 83.6 | f. Availability of Compensation clause to fall back upon in case of any breach of data (confidentiality, integrity, and availability), or incident that may result into any type of loss to PSB.  |  |  |  |

|      |  |  |  |  |
|------|--|--|--|--|
| 83.7 | g. No Sharing of data with any 3rd/4th party without explicit written permission from competent Information Owner of the Bank including with the Law Enforcement Agency (if applicable), etc.  |  |  |  |
| 84   | CERT IN Empaneled auditor report's is required for the following:  |  |  |  |
| 84.1 | a. CSP's environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by Firewall and any access from an external entity is permitted through DMZ only  |  |  |  |
| 84.2 | b. CSP follows the best practices of creation of separate network zones (VLAN segments) for Production and non-Production such as UAT  |  |  |  |
| 84.3 | c. Internet access is restricted on: Internal servers, database servers, Any other servers   |  |  |  |
| 84.4 | d. Ensuring security posture of their applications. Security Testing includes but is not limited to Appsec, API Testing, Source Code Review, VA, PT, SCD, DFRA, Process Review, Access Control etc.  |  |  |  |
| 84.5 | e. CSP has processes in place to permanently erase PSB data after processing or after a clearly defined retention period   |  |  |  |
| 84.6 | f. Log generation, storage, and review process to confirm whether proper log generation, storage, management, and analysis happens   |  |  |  |
| 84.7 | g. Whether the CSP has witnessed any security or privacy breach in the past 2 years  |  |  |  |
| 85   | Process and policies should be in place to stop and control data downloading. The same should be shared with bank on regular interval or as desired by bank.   |  |  |  |
| 86   | Data should not be allowed to be downloaded or to prepare copies unless explicitly approved by bank.   |  |  |  |
| 87   | Information security controls implemented by bidder and any third party (if any) must be at least as robust as those which the Bank would have implemented had the operations been performed in-house. Such implementation should cover all locations that support Bank's data storage and/ or processing requirements. Certificate of Assurance supported by suitable evidence should be submitted by bidder, regarding status of controls implemented at all locations. In case of a single evidence/report, assurance that controls are consistent across all relevant locations processing/storing Bank's data should be obtained. |  |  |  |
| 88   | Data must not be shared with outsiders without explicit & case specific approval of PSB. Data should not be allowed to be downloaded or to prepare copies unless explicitly approved.  |  |  |  |
| 89   | The key used by the vendor to encrypt PSB data should be different i.e., it should not be the same that was/is used for other clients  |  |  |  |
| 90   | CSP should ensure proper log generation, storage, management and analysis happens for the 3rd Party/Vendor application (including DFRA & access logs)  |  |  |  |
| 91   | CSP should have captive SOC or Managed Service SOC for monitoring their systems and operations   |  |  |  |
| 92   | Any/all decision pertaining to the proposed & provisioned applications and/or infrastructure and/or tools and/or services shall be obtained from PSB prior to provisioning   |  |  |  |
| 93   | The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB. Evidence of dedicated infrastructure (physical/logical) for PSB should be submitted.   |  |  |  |
| 94   | Rules are implemented on Firewalls of the 3rd Party/Vendor environment as per bidder approved process and rules & process are reviewed periodically.   |  |  |  |
| 95   | The Primary & secondary should be physically separate and should be at two different locations. Address of the same has to be provided in technical proposal   |  |  |  |
| 96   | Bidder should have in place procedures for emergency changes, including the roles and responsibilities, and that shall be documented.  |  |  |  |
| 97   | Mechanism shall be implemented for apprising details of sub-contracting of workload and periodically notifying changes in sub-contracting by CSP to Bank   |  |  |  |
| 98   | Bidder or CSP should have Risk Framework in place for cloud adoption shall include but not be limited to following checks:   |  |  |  |
| 98.1 | • Type of service being outsourced   |  |  |  |
| 98.2 | • Application criticality  |  |  |  |
| 98.3 | • Classification of data   |  |  |  |
| 98.4 | • Cloud service model  |  |  |  |
| 98.5 | • Cloud deployment model   |  |  |  |
| 98.6 | • Data localization requirements and Laws affecting cross-border data transfer and storage   |  |  |  |
| 98.7 | • Legal, regulatory and compliance requirements  |  |  |  |
| 98.8 | • Data availability and recovery requirements  |  |  |  |
| 98.9 | • Data recovery in case of disaster and in case of contract termination  |  |  |  |

|       |   |  |  |  |
|-------|---|--|--|--|
| 98.10 | <ul style="list-style-type: none"> <li>Feasibility to audit/review IT controls of the third party (CSP) or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.</li> </ul>  |  |  |  |
| 98.11 | <ul style="list-style-type: none"> <li>Global security practices</li> </ul>   |  |  |  |
| 98.12 | <ul style="list-style-type: none"> <li>Applicable threats, its likelihood and corresponding impact</li> </ul>   |  |  |  |
| 98.13 | <ul style="list-style-type: none"> <li>Data segregation, confidentiality, privacy controls at the third party (cloud)</li> <li>Sub-contracting</li> <li>continuous monitoring requirement</li> <li>Exit strategy</li> </ul>   |  |  |  |
| 99    | Bidder shall assist banks and provide all necessary documents and data for conducting Bidder's risk assessment during on boarding, periodically during life cycle and upon termination/transition of services.  |  |  |  |
| 100   | Threat Modelling of all activities being performed should be documented and should be shared with the bank on periodic basis  |  |  |  |
| 101   | Bidder's and CSP also confirms that bank reserve the right to Audit the premise/offices of any of its sub-contractor involved in the project as and when required by bank   |  |  |  |
|       | <b>Architecture</b>   |  |  |  |
| 102   | The architecture of the system should follow modular application architecture that emphasizes separating the functionality of applications in independent services. All the components of the application should have the ability to be reused and replaced without affecting the rest of the system fostering agility, efficiency, and resilience. |  |  |  |
| 103   | The system should support cloud delivery model as this approach will allow to redeploy parts of or all the application to a cloud platform, whenever required.  |  |  |  |
| 104   | The system must comply with organization's guiding principles & standards for enterprise information security/system architecture   |  |  |  |
| 105   | The system must be optimized to minimize their power and memory footprint for better performance  |  |  |  |
| 106   | Every design decision of the applications should take into account the optimum use of CPU, memory   |  |  |  |
| 107   | System must be designed to be efficient, scalable, manageable, fast, frugal with resources, composable and SOA-style self-contained   |  |  |  |
| 108   | The application architecture must be modular with different modules performing logically discrete functions, all modular services developed separately and composed together to construct an executable application program   |  |  |  |
| 109   | The data architecture must classify data in a number of ways: function, purpose, structure, confidentiality, sensitivity  |  |  |  |
| 110   | The solution should have a native support for cloud deployment model  |  |  |  |
| 111   | The solution should have detailed, periodically updated data dictionary   |  |  |  |
| 112   | Infrastructure diagrams, Security & network architecture, data flow diagrams, documentation and configurations must be up to date, controlled and available to assist in issue resolution.  |  |  |  |
|       | <b>Platform and Solution</b>  |  |  |  |
| 113   | The Bidder shall deploy the solution in dedicated cloud instance procured in the name of Bank for hosting the application.  |  |  |  |
| 114   | An administrator console to the bank to implement/manage/change organization level archival, retention and Backup policies.   |  |  |  |
| 115   | Browser software should support basic authentication, session authentication, active content filtering, additionally it should be designed to work well with supported proxy servers and virtual private network solutions  |  |  |  |
|       | <b>Scalability and Performance</b>  |  |  |  |
| 116   | The solution should support dynamic elasticity to cope up with the change in user loads.  |  |  |  |
| 117   | The solution should support horizontal and vertical scaling to meet the Bank's future requirement.  |  |  |  |
| 118   | Scaling process to be clearly defined by the Bidder and should not involve any code changes.  |  |  |  |
| 119   | The number of users who all are utilizing the Software Solution overall as well as at a given point in time should be available as a dashboard.   |  |  |  |
| 120   | Ability to scale linearly   |  |  |  |
| 121   | Solution should be able to scale to accommodate future usage loads, such as load balancing, clustering, support for additional CPU cores etc.   |  |  |  |
| 122   | Solution should meet performance standards regardless of the location within India  |  |  |  |
| 123   | Capability to handle sub second response time   |  |  |  |

|     |   |  |  |  |
|-----|---|--|--|--|
| 124 | Allow for high capacity to carry out transactions during high volume period   |  |  |  |
|     | <b>Security</b>   |  |  |  |
| 125 | The solution should comply with the security guidelines & principles of Bank, RBI and GOI   |  |  |  |
| 126 | Data should be protected at rest and in motion  |  |  |  |
| 127 | Secure mechanisms and protocols must be used for authentication   |  |  |  |
| 128 | When the application fails, it should fail to a state that rejects all subsequent security requests   |  |  |  |
| 129 | Every failure must be handled as per Risk Management Policy   |  |  |  |
| 130 | Application must be designed to recover to a known good state after an exception occurs   |  |  |  |
| 131 | A global error handler must be designed to catch unhandled exceptions and an appropriate logging and notification strategy must be designed   |  |  |  |
| 132 | Client account, transaction data or any sensitive information is encrypted when in transit.   |  |  |  |
| 133 | Solution should be implemented in higher security standards like Virtualization, Segregation of Servers, and compartmentalization. Secured Coding Practices, OWASP etc. to ensure 100% security of the Solution   |  |  |  |
| 134 | Solution should comply with the IT Security Policy, Cyber Security Policy, and IT Policy of the Bank  |  |  |  |
| 135 | Encryption to be used for API, data traveling between platform and other interfacing applications. Integrity of data to be maintained at 100% of time.  |  |  |  |
| 136 | The Bidder shall create adequate controls ensuring that, when exception or abnormal conditions occur, resulting errors do not allow users to bypass security checks or obtain core dumps.   |  |  |  |
| 137 | The solution should be compliant with DC/DR strategy of Bank  |  |  |  |
| 138 | All the components of proposed solution (software, etc.) in the Primary site should be replicable at the secondary site (except for test and development environment).  |  |  |  |
| 139 | The proposed solution should have full capability to support database- database and storage-storage replication between primary and secondary site with a recovery point objective (RPO) and a recovery time objective (RTO) of the Bank.   |  |  |  |
| 140 | The replication between Primary site and secondary site should be possible in both directions.  |  |  |  |
| 141 | Support real time replication of data from production site to secondary site and permit manual and automatic shift of the application to the secondary site.  |  |  |  |
|     | <b>Licensing and implementation requirements</b>  |  |  |  |
| 142 | The solution can be put to use bank branches/offices/locations  |  |  |  |
| 143 | The solution should be deployed in Development, Test, training and Production and there should not be any restriction on the number of instances / deployments / users based on the licenses and any other limitation quoted in Commercial Bid  |  |  |  |
|     | <b>Support and Maintenance</b>  |  |  |  |
| 144 | A request from the Bank to implement variants of the products already implemented shall not be treated as a change request / customization. And should be managed via configuration changes by the Bidder.  |  |  |  |
| 145 | Bidder should fix bugs identified during the period of contract at no additional cost to the Bank.  |  |  |  |
| 146 | Bidder should warrant all the software against defects arising out of faulty design, workmanship etc. throughout the contract period.   |  |  |  |
| 147 | Bidder should ensure availability of technical expertise and SMEs to extend continuous support to the on-site team.   |  |  |  |
| 148 | Bidder will be responsible to manage day-to-day operations, system administration & maintenance, system support, troubleshooting, technical support, patching, configuration, deployment, change & release management, and support (L1, L2 & L3) and cloud-based DR & BCP activities.   |  |  |  |
| 149 | Bidder should resume operations from an alternate site with minimum downtime whenever required  |  |  |  |
| 150 | Bidder in consultation with Bank will decide on the Change Requests (CR) to be taken up for coding and estimate the man days required for each CR and prepare a User Requirement Document (URD). After URD approval from Bank, Bidder team will start working on the CRs. If URD is not available, Bidder team will start working on the approved CR. |  |  |  |
| 151 | Bidder should perform system performance monitoring and publish uptime reports at the frequency desired by the Bank.  |  |  |  |
| 152 | Any change / upgrade / solution modification / patch suggested by the Bidder will be first communicated and discussed with the Bank; only after the confirmation and acceptance by the Bank shall it be applied to the production environment.  |  |  |  |
| 153 | Audit Trail - All transactions should be securely logged to detect any modifications.   |  |  |  |
| 154 | All historical records of deviation along with user audit trail should be logged for future reference.  |  |  |  |
| 155 | All overrides for credit approval or rejection should be logged to create audit trail that can be tracked.  |  |  |  |

|  |  |             |   |                            |
|--|--|-------------|---|----------------------------|
| 156                                    | History of each parameter change should be logged.   |             |   |                            |
| 157                                    | Users should be able to access audit trails of all the transactions, modifications/changes for audit purpose.  |             |   |                            |
| <b>Reporting</b>                       |  |             |   |                            |
| 158                                    | The system should support all the different reporting requirements of the Bank that includes MIS database instance,  |             |   |                            |
|  | § Customizable user specific reports   |             |   |                            |
|  | § Dashboard requirements   |             |   |                            |
|  | § Technical Audit Log trail reports for access control logs  |             |   |                            |
|  | § Reconciliatory reporting where needed  |             |   |                            |
|  | § System health check dashboard formonitoring health of application including security vulnerabilities.  |             |   |                            |
| <b>Performance Requirements</b>        |  |             |   |                            |
| 159                                    | Bank may engage any third-party solution for performance monitoring of the proposed solution for which the Bidder should support at no additional cost to Bank.  |             |   |                            |
| <b>Scalability Requirements</b>        |  |             |   |                            |
| 160                                    | Scaling process to be clearly defined by the Bidder and should not involve any code changes.   |             |   |                            |
| <b>Compliance with Bank's policies</b> |  |             |   |                            |
| 161                                    | The solution provider should not store or share any data outside the Bank's infrastructure.  |             |   |                            |
| 162                                    | <b>Ownership of data in the cloud</b> - CSP and/or bidder should have no rights or licenses, including without limitation intellectual property rights or licenses, to use data owned by Bank for its own purposes by virtue of the transaction or claim any security interest in data owned by Bank |             |   |                            |
| 163                                    | The solution should ensure that the log collection, storage, management, integrations are done in a secured and tamper proof manner and are within the Indian Jurisdiction.  |             |   |                            |
| 164                                    | Isolation of Banks data from other customers of CSP  |             |   |                            |
| 165                                    | Ownership of any/all data generated/fed/stored in the system lies with the bank and CSP has no rights or licenses or any IPR on the data.  |             |   |                            |
| 166                                    | Log retention should adhere to the time frame as per the Bank's log retention policy.  |             |   |                            |
| 167                                    | Data needs to be retained for a time frame as per the Bank's data retention policy.  |             |   |                            |
| 168                                    | Remote access from public domain / Bidder's workplace to Bank's environment will not be taken by the Bidder for any purpose including development, support operations, deployments, debugging etc.   |             |   |                            |
| 169                                    | Access to and disclosure of the Banks information assets by the CSP -Information should only be used by the CSP strictly for the purpose of the contracted service, and in accordance with the terms of pertaining to such use   |             |   |                            |
| 170                                    | Secure removal, return, retention and/ or destruction of assets and data belonging to Bank- Upon termination or upon the direction of the bank   |             |   |                            |
| 171                                    | CSP confirms and obligates himself to provide notification to the Bank in the event of any significant changes that may impact service availability (including controls and/or location) and security incidents i.e., breach of security or confidentiality (but not limited to)                     |             |   |                            |
| <b>Hardware</b>                        |  |             |   |                            |
| 172                                    | The solution should be deployed on dedicated cloud instance for Bank. The Bidder shall finalize the cloud solution requirement in line with volume, request/response times, cloud replication requirements, back up disk & media based.  |             |   |                            |
| 173                                    | The Bidder shall configure, deploy, support, and manage the set up for the Bank.   |             |   |                            |
| 174                                    | The bidder is required to ensure the storage of data in secured environment for the period as defined by bank. Once the services are discontinued by bank, the bidder & CSP must ensure that data is removed from all environments of CSP & bidder   |             |   |                            |
| <b>S. No.</b>                          | <b>Details of Control Point (Yes/No) Along with the required documentatry proof</b>  | <b>Area</b> | <b>Required Evidence</b>  | <b>Compliance (Yes/No)</b> |
| 175                                    | Whether the 3rd Party/Vendor/Vendor has (Board/Top Management approved) Information Security Policy in place with periodic reviews (Minimum annually) by Top Management?   | Governance  | Content Table/ Page of IS Policy and review history page  |                            |
| 176                                    | Whether IS Policy is communicated to all employees and does the entity monitor the compliance of the Policy?   | Governance  | Relevant evidence or Compliance Certificate   |                            |
| 177                                    | Whether the 3rd Party/Vendor has approved operational processes (SOP, etc.) with periodic review (at least annually) including but not limited to: Business Continuity Management, Backup Management and Restoration Testing, Desktop/system/server/network device hardening with Baseline controls  |             | For organizations with ISO-27001, PCI-DSS, SOC1, SOC2 certifications, relevant certification with validity period needs to be produced. |                            |

|     |  |                  |   |  |
|-----|--|------------------|---|--|
| 178 | and restoration testing, Desktop/system/server/network device hardening with baseline controls, Patch Management, Port Management, Media Movement, Log Management, Personnel Security, Physical Security, Internal Security Assessment Processes, Incident Management, Regulatory Compliance | Governance       | For other organizations, each approved document/IS Policy (respective contents) needs to be produced with version history. (Sample evidence verification for non-Govt entity) |  |
| 179 | Whether the 3rd Party/Vendor has deployed a dedicated information security team independent of IT, reporting directly to MD/CIO for conducting security related functions & operations?  | Governance       | Relevant clauses in Policy and implementation evidence like organization structure etc.   |  |
| 180 | Whether suitable Security certifications (ISO, PCI-DSS, SOC1 and SOC2 etc) of the security posture at vendor environment are in place?   | Governance       | Certificate with validity period, if available.   |  |
| 181 | Wherever any work or part of work is outsourced by the Third Party to any other party(subletting), whether the Security prescriptions of the Fourth Party are reviewed/ensured to be equivalent to those of the third Party?   | Governance       | SLA Clause and Self Certification of having reviewed the systems of sub-letting entity by vendor i.e., 3rd party.   |  |
| 182 | Whether required approvals are in place for sharing data with third party?   | Governance       | IT-AO to obtain approval of the Appropriate Authority & keep as evidence. (Action Owner -IT AO)   |  |
| 183 | 3rd Party/Vendor/Any sub-contractor of the vendor shall allow the following:   | Governance       |   |  |
| 184 | -Right to Audit to PSB with scope defined.   |                  |   |  |
| 185 | -Right to recall data by PSB.  |                  |   |  |
| 186 | -System of taking approvals for making changes in the application.   |                  |   |  |
| 187 | -Regulatory and Statutory compliance at vendor site.   |                  |   |  |
| 188 | -Special emphasis on IT Act 2000 & its amendments, and other Acts/Regulatory guidelines?   |                  |   |  |
| 189 | -Availability of Compensation clause to fall back upon in case of any breach of data (confidentiality, integrity, and availability), or incident that may result into any type of loss to PSB.   |                  |   |  |
| 190 | -No Sharing of data with any 3rd/4th party without explicit written permission from competent Information Owner of the Bank including with the Law Enforcement Agency (if applicable), etc.  |                  |   |  |
| 191 | -Residual risk to be covered by incorporating suitable legal terms in SLA.   |                  |   |  |
| 192 | Whether background verification of the officials of the vendor, CSP and its third party is completed before onboarding?  | Human Resource   | Employee recruitment process, Sample evidence to be submitted   |  |
| 193 |  | Security         |   |  |
| 194 | Whether privilege access to the 3rd Party/Vendor environment is permitted from internet?   | Access           | Evidence for the secured access, reviewed by CERT empaneled auditors.   |  |
| 195 |  | Management       |   |  |
| 196 | Whether the 3rd Party/Vendor configures or provides access to officials based on a documented and approved Role Conflict Matrix?   | Access           | Role Conflict Matrix and evidence of following the same.  |  |
| 197 |  | Management       |   |  |
| 198 | Whether all default admin and root users are deleted/disabled, and access is based on user specific IDs and all such accesses are logged.  | Access           | Evidence of having disabled default admins and root users   |  |
| 199 |  | Management       | preferably verified by CERT empaneled auditor.  |  |
| 200 | Whether the third party has deployed Active Directory (AD), Single Sign On (SSO) and strong Password Policy for End point and application access?  | Access           | Details of the AD, SSO, Password Policy in relevant clauses of IS Policy and/or compliance verification..   |  |
| 201 |  | Management       |   |  |
| 202 | Whether proper access control is defined for protecting PSB data and access to the Data is strictly on Need-to-Know Basis?   | Access           | Approved Access Control process document and evidence of implementation   |  |
| 203 |  | Management       |   |  |
| 204 | Whether the 3rd Party/Vendor's environment is suitably protected from external threats by way of firewall, IDS/IPS, AV, DLP etc. ?   | Network Security | Evidence for controls in place  |  |
| 205 | Whether the 3rd Party/Vendor's environment is suitably protected from external threats by way of WAF, NAC etc. ?   | Network Security | Evidence for controls in place  |  |
| 206 | Whether rules are implemented on Firewalls of the 3rd Party/Vendor environment as per their approved process? Whether the entity has an approved process for regular reviews and updates   | Network Security | Approved Process of Firewall Rules and self-certification (signed by IS Head of the company) for non-presence of overly permissible rules                                     |  |
| 207 | Whether the 3rd Party/Vendor environment is segregated into militarized zone (MZ) and demilitarized zone (DMZ) separated by Firewall, where any access from an external entity is permitted through DMZ only?  | Network Security | CERT empaneled auditor's Report on verification of its implementation.  |  |
| 208 | Whether the 3rd Party/Vendor follows the best practices of creation of separate network zones (VLAN segments) for Production and non production such as UAT  | Network Security | CERT empaneled auditor's Report on verification of its implementation.  |  |
| 209 | Whether the 3rd Party/Vendor follows the best practices of creation of separate network zones (VLAN segments) for Web, App, DB, Critical & Non-Critical Applications   | Network Security | Self-certification (signed by IS Head of the company) with evidence.  |  |

|     |   |                               |   |  |
|-----|---|-------------------------------|---|--|
| 210 | Whether third party has a separate network architecture diagram specific to integration with PSB  | Network Security              | Network architecture diagram specific to PSB  |  |
| 211 | Whether Internet access is restricted on:   | Network Security              | Evidence of purpose/need of this and verification of controls in place by CERT empaneled ISSP.  |  |
| 212 | -Internal servers   |                               |   |  |
| 213 | -Database servers   |                               |   |  |
| 214 | -Any other servers?   |                               |   |  |
| 215 | The application and DB is/will be hosted separately on a dedicated infrastructure (physical/logical) for PSB  | Network Security              | Evidence of dedicated infrastructure (physical/logical) for PSB   |  |
| 216 | Whether CERT Empaneled Auditors are engaged by the third party for ensuring security posture of their applications? Security Testing includes but is not limited to Appsec, API Testing, Source Code Review, VA, PT, SCD, DFRA, Process Review, Access Control etc. | Application Security          | Latest security Testing Certification with Scope of review & closure of observations.   |  |
| 217 | Whether the 3rd Party/Vendor has deployed any open source or free software in their environment? If yes, whether processes are in place for closure of vulnerabilities & regular/timely patching for such software?   | Application Security          | If any Open Source software is used, evidence for process in place to adhere to the stated control and/or declaration that there are no known CVE (Common Vulnerability & Exposures)  |  |
| 218 | Whether minimum baseline controls are implemented for hardening the Application and DB Servers?   | Application Security          | Content page of SCD document and review history and implementation evidence of latest SCD version   |  |
| 219 | Where PSB Data is permitted & required to be shared, whether only the bare minimum data is being shared? (Please document the NEED for sharing every data field)  | Data Security                 | IT-AO to obtain approval of the Appropriate Authority, and keep as evidence, specifying data elements shared (Action Owner -IT AO)  |  |
| 220 | Whether the 3rd Party/Vendor is permitted & required to store the data owned by PSB? If so, whether relevant approval to that effect is obtained ? What are the security measures for safe storage and timely retrieval of data?                                    | Data Security                 | IT-AO to obtain approval of the Appropriate Authority for PSB Data storage at 3rd Party & related aspects i.e. security, period, purging, monitoring, etc; and keep both approval & implementation as evidences. (Action Owner - IT AO) |  |
| 221 | Whether the 3rd Party/Vendor is permitted to outsource the activity or share PSB specific data to any other party, partly or fully, for any purpose? If so, are the specific activities / data elements and purpose documented and are made part of SLA ?           | Data Security                 | Specify in SLA Clause. (Action Owner -IT AO)  |  |
| 222 | Whether the 3rd Party/Vendor is permitted to take any crucial decisions on behalf of PSB without specific written approval from the IT  | Data Security                 | Specify in SLA Clause and obtain Self Certification. (Action Owner -IT AO)  |  |
| 223 | Whether Suitable Security certificate such as ISO27017 & ISO27018 for Cloud Services and PCI DSS where Debit Card related data are stored   | Data Security                 | Certificate with validity period.   |  |
| 224 | Whether the data shared by PSB secured while transit, processing, at store, during backup and Archivals, over external media etc. with latest & secured encryption standards?   | Data Security                 | Evidence for protection of data in transit such as Secure Encryption algorithm used   |  |
| 225 | Whether processes are in place to permanently erase PSB data after processing or after a clearly defined retention period by the 3rd Party/Vendor? How this will be monitored?  | Data Security                 | Self-certification in case of Govt entity and Approved Purging Process & timeline and Evidence of actual implementation for non-Govt entities duly verified by CERT empaneled IS auditor  |  |
| 226 | Data must not be shared with outsiders without explicit & case specific approval of PSB   | Data Security                 | SLA Clause and periodic Self Certification  |  |
| 227 | The key used by the vendor to encrypt PSB data should be different i.e. it should not be the same that was/is used for other clients.   | Data Security                 | Approved Process for Key Mgmt. and Evidence of actual implementation of Key Sharing   |  |
| 228 | Data should not be allowed to be downloaded or to prepare copies unless explicitly approved.  | Data Security                 | Approved Process & Evidence of implementation of the control.   |  |
| 229 | Whether the application and database (containing PSB data) is hosted in Public Cloud?   | Cloud Security                | Approval from IT-AO for the requirement in line with Bank's IS Policy. Approved Document on Cloud Security & its implementation. Or ISO 27017&18 Certificate  |  |
| 230 | Whether proper log generation, storage, management and analysis happens for the 3rd Party/Vendor application (including DFRA & access logs) ?   | Log Management and Monitoring | Log generation, storage and review process certified by CERT empaneled auditor.   |  |
| 231 | Whether the privilege access activities are logged, monitored, controlled and governed preferably using Privilege Identity Management (PIM)   | Log Management and Monitoring | Evidence of Privileged access logs and PIMS implementation  |  |
| 232 | Whether the 3rd Party/Vendor has captive SOC or Managed Service SOC for monitoring their systems and operations?  | Log Management and Monitoring | Evidence of SOC implementation and its activities   |  |
| 233 | Whether the 3rd Party Vendor has witnessed any security or privacy breach in the past 2 years?  | Incident Response             | Self certification of IS Head in case of Govt entity/evidence reported to Regulatory agencies and/or self attestation and the same to be verified by CERT empaneled ISSP.   |  |



|     |  |                     |  |  |
|-----|--|---------------------|--|--|
| 234 | Whether 3rd Party/Vendor has deployed secure environments for the proposed applications  | Business Continuity | Evidence of a Secured DR Site at different location(s).  |  |
| 235 | Whether the Vendor performs periodic DR Drills?  | Business Continuity | Evidence of conducting DR drills, and lessons learnt and their detailed recordings.  |  |
| 236 | Is the mechanism to separate and secure data from other tenets is in place? May be by Firewalls rule   |                     | Required process/proof to  |  |
| 237 | implementation.  |                     | be submitted   |  |
| 238 | Whether Information Security Auditors are engaged by Cloud Provider for ensuring security posture of their cloud. Security testing includes but is not limited to APPSEC, API Testing, Source Code Review, VA, PT, SCD, DFRA, Process Review, Access Control etc.  |                     | Latest security Testing Certification with Scope of review & closure of observations.  |  |
| 239 | Whether a system is in place to inform any changes in the cloud environment  |                     | Certification/Documentation to be shared   |  |
| 240 | Whether Control mechanism such as Active Directory (AD), Single Sign On (SSO) and strong Password Policy for End point and application access can be deployed in Public Cloud Provider?  |                     | Evidence of the mechanism  |  |
| 241 | Does Cloud Provider provide that internet access is restricted on internal servers, database servers or any other servers.   |                     | Evidence of the mechanism  |  |
| 242 | Whether Cloud Provider is using any open source or free software in their environment. If yes, whether processes are in place for closure of vulnerabilities & regular/timely patching for such software.  |                     | If any Open-Source software is used, evidence for process in place to adhere to the stated control and/or declaration that there are no known CVE (Common Vulnerability & Exposures).  |  |
| 243 | Whether Cloud Provider has the controls that data should not be allowed to be downloaded or to prepare copies by Cloud Provider, unless explicitly approved BY BANK.   |                     | Evidence of the mechanism  |  |
| 244 | Whether third party conducts security Assessment of all their applications (PSB related) covering activities (including not limited to) Appsec, API Testing, Source Code Review, DFRA, Process Review, Vulnerability Assessment, Penetration Testing, Internal and External APIs, DB Review etc through regulator/ government (CERT empanelled or others) approved auditors.   |                     | Evidence of latest Security Reports by Govt / Regulator approved / CERT empanelled auditors  |  |
| 245 | The Review should also cover all components used in the Docker Security, Orchestration Software security, Storage Security, Effective implementation, and Proper configuration of Security Tools such as WAF, DLP, IRM, PIMS etc should also be in scope.  |                     |  |  |
| 246 | Whether Secure Network architecture covering the following is in place Networking / Routing within the Cloud Networking/ Routing outside to the Cloud environment (Ingress / Egress connections) VPC provisioning / Mechanisms to avoid Lateral access Network segregation amongst various environments (Dev/ UAT/ Prod etc)(and DMZ/MZ Zones Whether Cloud Storage is accessible only through VPC and not directly through internet |                     | Evidence of latest Security Reports by Govt / Regulator approved / CERT empanelled auditors.   |  |
| 247 | Whether Security of the data throughout Data Lifecycle is ensured and evidenced  |                     | Evidence of latest Security Reports by Govt / Regulator approved / CERT empanelled auditors.   |  |
| 248 | Whether secured Key Management process is in place.  |                     | Evidence of latest Security Reports by Govt / Regulator approved / CERT empanelled auditors. If BYOK is not evidenced, explicit controls to avoid comingling and Key Mgmt. Lifecycle to be ensured and certified in the audit. |  |

# PUNJAB & SIND BANK



## REQUEST FOR PROPOSAL

FOR

SELECTION OF BIDDER FOR SUPPLY INSTALLATION, IMPLEMENTATION,  
MAINTENANCE & MANAGEMENT OF IT SECURITY SOLUTIONS - B

BID NO: PSB/HOIT/RFP/2025-26/45 DATED 01/10/2025

## APPENDIX 3: Bill of Quantity

HEAD OFFICE IT DEPARTMENT

2ND FLOOR,

PLOT NO. 151, SECTOR 44

INSTITUTIONAL AREA, GURUGRAM -122003

| Component | DC             |                      |      |       |                       |                                |                     |                         |                       |   |
|-----------|----------------|----------------------|------|-------|-----------------------|--------------------------------|---------------------|-------------------------|-----------------------|---|
| S.No.     | BoQ Reference  | Qty of proposed Item | Make | Model | Name of the processor | Number of processor per server | Cores per processor | Memory per server in GB | DIMM Slots per server | HDD per server (Usable before de-dupe & compression ) in GB |
| 1         | Server Model 1 |                      |      |       |                       |                                |                     |                         |                       |   |
| 2         | Server Model 2 |                      |      |       |                       |                                |                     |                         |                       |   |
| 3         | Server Model 3 |                      |      |       |                       |                                |                     |                         |                       |   |
| 4         | Server Model 4 |                      |      |       |                       |                                |                     |                         |                       |   |
| 5         | Server Model 5 |                      |      |       |                       |                                |                     |                         |                       |   |

| Component | Primary Storage (PS) |                      |      |       |   |                                  |   |   |               |  |
|-----------|----------------------|----------------------|------|-------|---|----------------------------------|---|---|---------------|--|
| S.No.     | BoQ Reference        | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of controller per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1         | PS Model 1           |                      |      |       |   |                                  |   |   |               |  |
| 2         | PS Model 2           |                      |      |       |   |                                  |   |   |               |  |
| 3         | PS Model 3           |                      |      |       |   |                                  |   |   |               |  |
| 4         | PS Model 4           |                      |      |       |   |                                  |   |   |               |  |
| 5         | PS Model 5           |                      |      |       |   |                                  |   |   |               |  |

| Component | Object Storage (OS) |                      |      |       |   |                           |   |   |               |  |
|-----------|---------------------|----------------------|------|-------|---|---------------------------|---|---|---------------|--|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of CPU per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1         | OS Model 1          |                      |      |       |   |                           |   |   |               |  |
| 2         | OS Model 2          |                      |      |       |   |                           |   |   |               |  |
| 3         | OS Model 3          |                      |      |       |   |                           |   |   |               |  |
| 4         | OS Model 4          |                      |      |       |   |                           |   |   |               |  |
| 5         | OS Model 5          |                      |      |       |   |                           |   |   |               |  |

| Component | SAN Switch (SAN S/W) |                      |      |       |                                      |                                      |   |  |   |  |
|-----------|----------------------|----------------------|------|-------|--------------------------------------|--------------------------------------|---|--|---|--|
| S.No.     | BoQ Reference        | Qty of proposed Item | Make | Model | Number of Ports available per switch | Number of switch licensed per switch | Qty of port with 32 GBps & backward compatible to 8/16 Gbps | Qty of port with 16 GBps & backward compatible to 8/4 Gbps | Qty of licensed port with 32 GBps & backward compatible to 8/16 Gbps and Qty of proposed SFPs | Qty of licensed port with 16 GBps & backward compatible to 8/4 Gbps and Qty of proposed SFPs |
| 1         | SAN S/W Model 1      |                      |      |       |                                      |                                      |   |  |   |  |
| 2         | SAN S/W Model 2      |                      |      |       |                                      |                                      |   |  |   |  |
| 3         | SAN S/W Model 3      |                      |      |       |                                      |                                      |   |  |   |  |
| 4         | SAN S/W Model 4      |                      |      |       |                                      |                                      |   |  |   |  |
| 5         | SAN S/W Model 5      |                      |      |       |                                      |                                      |   |  |   |  |

| Component | Long Term Storage |                      |      |       |   |                           |   |   |               |  |
|-----------|-------------------|----------------------|------|-------|---|---------------------------|---|---|---------------|--|
| S.No.     | BoQ Reference     | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of CPU per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1         | LTS Model 1       |                      |      |       |   |                           |   |   |               |  |
| 2         | LTS Model 2       |                      |      |       |   |                           |   |   |               |  |
| 3         | LTS Model 3       |                      |      |       |   |                           |   |   |               |  |
| 4         | LTS Model 4       |                      |      |       |   |                           |   |   |               |  |
| 5         | LTS Model 5       |                      |      |       |   |                           |   |   |               |  |

| Component | APPLIANCES    |               |      |       |                       |                                |                                 |                           |  |  |
|-----------|---------------|---------------|------|-------|-----------------------|--------------------------------|---------------------------------|---------------------------|--|--|
| S.No.     | BoQ Reference | Solution Name | Make | Model | Name of the Appliance | Configuration of the appliance | Additioant features and details | Quantity of the appliance |  |  |
| 1         | APPLIANCE 1   |               |      |       |                       |                                |                                 |                           |  |  |
| 2         | APPLIANCE 2   |               |      |       |                       |                                |                                 |                           |  |  |
| 3         | APPLIANCE 3   |               |      |       |                       |                                |                                 |                           |  |  |
| 4         | APPLIANCE 4   |               |      |       |                       |                                |                                 |                           |  |  |
| 5         | APPLIANCE 5   |               |      |       |                       |                                |                                 |                           |  |  |
| 6         | APPLIANCE 6   |               |      |       |                       |                                |                                 |                           |  |  |
| 7         | APPLIANCE 7   |               |      |       |                       |                                |                                 |                           |  |  |
| 8         | APPLIANCE 8   |               |      |       |                       |                                |                                 |                           |  |  |
| 9         | APPLIANCE 9   |               |      |       |                       |                                |                                 |                           |  |  |
| 10        | APPLIANCE 10  |               |      |       |                       |                                |                                 |                           |  |  |

| Component | IT Infra Supporting Software |
|-----------|------------------------------|
|-----------|------------------------------|

| Component | Operating System (OS) |                      |      |       |         |         |                   |
|-----------|-----------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | OS Model 1            |                      |      |       |         |         |                   |
| 2         | OS Model 2            |                      |      |       |         |         |                   |
| 3         | OS Model 3            |                      |      |       |         |         |                   |
| 4         | OS Model 4            |                      |      |       |         |         |                   |

| Component | Application server software (ASS) |                      |      |       |         |         |                   |
|-----------|-----------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                     | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | ASS Model 1                       |                      |      |       |         |         |                   |
| 2         | ASS Model 2                       |                      |      |       |         |         |                   |
| 3         | ASS Model 3                       |                      |      |       |         |         |                   |
| 4         | ASS Model 4                       |                      |      |       |         |         |                   |

| Component | Web Server software (WSS) |                      |      |       |         |         |                   |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |

|   |             |  |  |  |  |  |  |
|---|-------------|--|--|--|--|--|--|
| 1 | WSS Model 1 |  |  |  |  |  |  |
| 2 | WSS Model 2 |  |  |  |  |  |  |
| 3 | WSS Model 3 |  |  |  |  |  |  |
| 4 | WSS Model 4 |  |  |  |  |  |  |

| Component | Backup Software |                      |      |       |         |         |                   |
|-----------|-----------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | BS Model 1      |                      |      |       |         |         |                   |
| 2         | BS Model 2      |                      |      |       |         |         |                   |
| 3         | BS Model 3      |                      |      |       |         |         |                   |
| 4         | BS Model 4      |                      |      |       |         |         |                   |

| Component | Virtualization/Containerization/HCI |                      |      |       |         |         |                   |
|-----------|-------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | VCH Model 1                         |                      |      |       |         |         |                   |
| 2         | VCH Model 2                         |                      |      |       |         |         |                   |
| 3         | VCH Model 3                         |                      |      |       |         |         |                   |
| 4         | VCH Model 4                         |                      |      |       |         |         |                   |

| Component | Database      |                      |      |       |         |         |                   |
|-----------|---------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | DB Model 1    |                      |      |       |         |         |                   |
| 2         | DB Model 2    |                      |      |       |         |         |                   |
| 3         | DB Model 3    |                      |      |       |         |         |                   |
| 4         | DB Model 4    |                      |      |       |         |         |                   |

| Component | DR             |                      |      |       |                       |                                |                     |                         |                       |   |
|-----------|----------------|----------------------|------|-------|-----------------------|--------------------------------|---------------------|-------------------------|-----------------------|---|
| Component | Server         |                      |      |       |                       |                                |                     |                         |                       |   |
| S.No.     | BoQ Reference  | Qty of proposed Item | Make | Model | Name of the processor | Number of processor per server | Cores per processor | Memory per server in GB | DIMM Slots per server | HDD per server (Usable before de-dupe & compression ) in GB |
| 1         | Server Model 1 |                      |      |       |                       |                                |                     |                         |                       |   |
| 2         | Server Model 2 |                      |      |       |                       |                                |                     |                         |                       |   |
| 3         | Server Model 3 |                      |      |       |                       |                                |                     |                         |                       |   |
| 4         | Server Model 4 |                      |      |       |                       |                                |                     |                         |                       |   |
| 5         | Server Model 5 |                      |      |       |                       |                                |                     |                         |                       |   |

| Component | Primary Storage (PS) |                      |      |       |   |                                  |   |   |               |  |
|-----------|----------------------|----------------------|------|-------|---|----------------------------------|---|---|---------------|--|
| S.No.     | BoQ Reference        | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of controller per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1         | PS Model 1           |                      |      |       |   |                                  |   |   |               |  |
| 2         | PS Model 2           |                      |      |       |   |                                  |   |   |               |  |
| 3         | PS Model 3           |                      |      |       |   |                                  |   |   |               |  |
| 4         | PS Model 4           |                      |      |       |   |                                  |   |   |               |  |
| 5         | PS Model 5           |                      |      |       |   |                                  |   |   |               |  |

| Component | Object Storage (OS) |                      |      |       |   |                           |   |   |               |  |
|-----------|---------------------|----------------------|------|-------|---|---------------------------|---|---|---------------|--|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of CPU per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1         | OS Model 1          |                      |      |       |   |                           |   |   |               |  |
| 2         | OS Model 2          |                      |      |       |   |                           |   |   |               |  |
| 3         | OS Model 3          |                      |      |       |   |                           |   |   |               |  |
| 4         | OS Model 4          |                      |      |       |   |                           |   |   |               |  |
| 5         | OS Model 5          |                      |      |       |   |                           |   |   |               |  |

| Component | SAN Switch (SAN S/W) |                      |      |       |                                      |                                      |   |  |   |  |
|-----------|----------------------|----------------------|------|-------|--------------------------------------|--------------------------------------|---|--|---|--|
| S.No.     | BoQ Reference        | Qty of proposed Item | Make | Model | Number of Ports available per switch | Number of switch licensed per switch | Qty of port with 32 GBps & backward compatible to 8/16 Gbps | Qty of port with 16 GBps & backward compatible to 8/4 Gbps | Qty of licensed port with 32 GBps & backward compatible to 8/16 Gbps and Qty of proposed SFPs | Qty of licensed port with 16 GBps & backward compatible to 8/4 Gbps and Qty of proposed SFPs |
| 1         | SAN S/W Model 1      |                      |      |       |                                      |                                      |   |  |   |  |
| 2         | SAN S/W Model 2      |                      |      |       |                                      |                                      |   |  |   |  |
| 3         | SAN S/W Model 3      |                      |      |       |                                      |                                      |   |  |   |  |
| 4         | SAN S/W Model 4      |                      |      |       |                                      |                                      |   |  |   |  |
| 5         | SAN S/W Model 5      |                      |      |       |                                      |                                      |   |  |   |  |

| Component | Long Term Storage |                      |      |       |   |                           |  |   |               |  |
|-----------|-------------------|----------------------|------|-------|---|---------------------------|--|---|---------------|--|
| S.No.     | BoQ Reference     | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of CPU per storage | Proposed Usable capacity before dedupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1         | LTS Model 1       |                      |      |       |   |                           |  |   |               |  |
| 2         | LTS Model 2       |                      |      |       |   |                           |  |   |               |  |
| 3         | LTS Model 3       |                      |      |       |   |                           |  |   |               |  |
| 4         | LTS Model 4       |                      |      |       |   |                           |  |   |               |  |
| 5         | LTS Model 5       |                      |      |       |   |                           |  |   |               |  |

| Component | APPLIANCES    |               |      |       |                       |                                |                                 |                           |  |  |
|-----------|---------------|---------------|------|-------|-----------------------|--------------------------------|---------------------------------|---------------------------|--|--|
| S.No.     | BoQ Reference | Solution Name | Make | Model | Name of the Appliance | Configuration of the appliance | Additioanl features and details | Quantity of the appliance |  |  |
| 1         | APPLIANCE 1   |               |      |       |                       |                                |                                 |                           |  |  |
| 2         | APPLIANCE 2   |               |      |       |                       |                                |                                 |                           |  |  |
| 3         | APPLIANCE 3   |               |      |       |                       |                                |                                 |                           |  |  |

|    |              |  |  |  |  |  |  |  |  |  |
|----|--------------|--|--|--|--|--|--|--|--|--|
| 4  | APPLIANCE 4  |  |  |  |  |  |  |  |  |  |
| 5  | APPLIANCE 5  |  |  |  |  |  |  |  |  |  |
| 6  | APPLIANCE 6  |  |  |  |  |  |  |  |  |  |
| 7  | APPLIANCE 7  |  |  |  |  |  |  |  |  |  |
| 8  | APPLIANCE 8  |  |  |  |  |  |  |  |  |  |
| 9  | APPLIANCE 9  |  |  |  |  |  |  |  |  |  |
| 10 | APPLIANCE 10 |  |  |  |  |  |  |  |  |  |

**Component** IT Intra Supporting Software

| Operating System (OS) |               |                      |      |       |         |         |                   |  |
|-----------------------|---------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.                 | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1                     | OS Model 1    |                      |      |       |         |         |                   |  |
| 2                     | OS Model 2    |                      |      |       |         |         |                   |  |
| 3                     | OS Model 3    |                      |      |       |         |         |                   |  |
| 4                     | OS Model 4    |                      |      |       |         |         |                   |  |

| Application server software (ASS) |               |                      |      |       |         |         |                   |  |
|-----------------------------------|---------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.                             | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1                                 | ASS Model 1   |                      |      |       |         |         |                   |  |
| 2                                 | ASS Model 2   |                      |      |       |         |         |                   |  |
| 3                                 | ASS Model 3   |                      |      |       |         |         |                   |  |
| 4                                 | ASS Model 4   |                      |      |       |         |         |                   |  |

| Web Server software (WSS) |               |                      |      |       |         |         |                   |  |
|---------------------------|---------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.                     | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1                         | WSS Model 1   |                      |      |       |         |         |                   |  |
| 2                         | WSS Model 2   |                      |      |       |         |         |                   |  |
| 3                         | WSS Model 3   |                      |      |       |         |         |                   |  |
| 4                         | WSS Model 4   |                      |      |       |         |         |                   |  |

| Backup Software |               |                      |      |       |         |         |                   |  |
|-----------------|---------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.           | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1               | BS Model 1    |                      |      |       |         |         |                   |  |
| 2               | BS Model 2    |                      |      |       |         |         |                   |  |
| 3               | BS Model 3    |                      |      |       |         |         |                   |  |
| 4               | BS Model 4    |                      |      |       |         |         |                   |  |

| Virtualization/Containerization/HCI |               |                      |      |       |         |         |                   |  |
|-------------------------------------|---------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.                               | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1                                   | VCH Model 1   |                      |      |       |         |         |                   |  |
| 2                                   | VCH Model 2   |                      |      |       |         |         |                   |  |
| 3                                   | VCH Model 3   |                      |      |       |         |         |                   |  |
| 4                                   | VCH Model 4   |                      |      |       |         |         |                   |  |

| Database |               |                      |      |       |         |         |                   |  |
|----------|---------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.    | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1        | DB Model 1    |                      |      |       |         |         |                   |  |
| 2        | DB Model 2    |                      |      |       |         |         |                   |  |
| 3        | DB Model 3    |                      |      |       |         |         |                   |  |
| 4        | DB Model 4    |                      |      |       |         |         |                   |  |

| NON-PRODUCTION |                |                      |      |       |                       |                                |                     |                         |                       |   |
|----------------|----------------|----------------------|------|-------|-----------------------|--------------------------------|---------------------|-------------------------|-----------------------|---|
| Server         |                |                      |      |       |                       |                                |                     |                         |                       |   |
| S.No.          | BoQ Reference  | Qty of proposed Item | Make | Model | Name of the processor | Number of processor per server | Cores per processor | Memory per server in GB | DIMM Slots per server | HDD per server (Usable before de-dupe & compression ) in GB |
| 1              | Server Model 1 |                      |      |       |                       |                                |                     |                         |                       |   |
| 2              | Server Model 2 |                      |      |       |                       |                                |                     |                         |                       |   |
| 3              | Server Model 3 |                      |      |       |                       |                                |                     |                         |                       |   |
| 4              | Server Model 4 |                      |      |       |                       |                                |                     |                         |                       |   |
| 5              | Server Model 5 |                      |      |       |                       |                                |                     |                         |                       |   |

| Primary Storage (PS) |               |                      |      |       |   |                                  |   |   |               |  |
|----------------------|---------------|----------------------|------|-------|---|----------------------------------|---|---|---------------|--|
| S.No.                | BoQ Reference | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of controller per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1                    | PS Model 1    |                      |      |       |   |                                  |   |   |               |  |
| 2                    | PS Model 2    |                      |      |       |   |                                  |   |   |               |  |
| 3                    | PS Model 3    |                      |      |       |   |                                  |   |   |               |  |
| 4                    | PS Model 4    |                      |      |       |   |                                  |   |   |               |  |
| 5                    | PS Model 5    |                      |      |       |   |                                  |   |   |               |  |

| Object Storage (OS) |               |                      |      |       |   |                           |   |   |               |  |
|---------------------|---------------|----------------------|------|-------|---|---------------------------|---|---|---------------|--|
| S.No.               | BoQ Reference | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of CPU per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1                   | OS Model 1    |                      |      |       |   |                           |   |   |               |  |
| 2                   | OS Model 2    |                      |      |       |   |                           |   |   |               |  |
| 3                   | OS Model 3    |                      |      |       |   |                           |   |   |               |  |
| 4                   | OS Model 4    |                      |      |       |   |                           |   |   |               |  |
| 5                   | OS Model 5    |                      |      |       |   |                           |   |   |               |  |

**Component** SAN Switch (SAN S/W)

| S.No. | BoQ Reference   | Qty of proposed Item | Make | Model | Number of Ports available per switch | Number of switch licensed per switch | Qty of port with 32 Gbps & backward compatible to 8/16 Gbps | Qty of port with 16 Gbps & backward compatible to 8/4 Gbps | Qty of licensed port with 32 Gbps & backward compatible to 8/16 Gbps and Qty of proposed SFPs | Qty of licensed port with 16 Gbps & backward compatible to 8/4 Gbps and Qty of proposed SFPs |
|-------|-----------------|----------------------|------|-------|--------------------------------------|--------------------------------------|---|--|---|--|
| 1     | SAN S/W Model 1 |                      |      |       |                                      |                                      |   |  |   |  |
| 2     | SAN S/W Model 2 |                      |      |       |                                      |                                      |   |  |   |  |
| 3     | SAN S/W Model 3 |                      |      |       |                                      |                                      |   |  |   |  |
| 4     | SAN S/W Model 4 |                      |      |       |                                      |                                      |   |  |   |  |
| 5     | SAN S/W Model 5 |                      |      |       |                                      |                                      |   |  |   |  |

| Component | Long Term Storage |                      |      |       |   |                           |   |   |               |  |
|-----------|-------------------|----------------------|------|-------|---|---------------------------|---|---|---------------|--|
| S.No.     | BoQ Reference     | Qty of proposed Item | Make | Model | IOPS per storage (@8 KB block size, 60% read & 40% write) | Number of CPU per storage | Proposed Usable capacity before de-dupe & compression ) in GB | Number of Drives (data & parity) and raw capacity of each drive | FC Port Speed | Scalability supported (Usable Capacity by addition of additional drives) |
| 1         | LTS Model 1       |                      |      |       |   |                           |   |   |               |  |
| 2         | LTS Model 2       |                      |      |       |   |                           |   |   |               |  |
| 3         | LTS Model 3       |                      |      |       |   |                           |   |   |               |  |
| 4         | LTS Model 4       |                      |      |       |   |                           |   |   |               |  |
| 5         | LTS Model 5       |                      |      |       |   |                           |   |   |               |  |

| Component | APPLIANCES    |               |      |       |                       |                                |                                 |                           |  |  |
|-----------|---------------|---------------|------|-------|-----------------------|--------------------------------|---------------------------------|---------------------------|--|--|
| S.No.     | BoQ Reference | Solution Name | Make | Model | Name of the Appliance | Configuration of the appliance | Additioanl features and details | Quantity of the appliance |  |  |
| 1         | APPLIANCE 1   |               |      |       |                       |                                |                                 |                           |  |  |
| 2         | APPLIANCE 2   |               |      |       |                       |                                |                                 |                           |  |  |
| 3         | APPLIANCE 3   |               |      |       |                       |                                |                                 |                           |  |  |
| 4         | APPLIANCE 4   |               |      |       |                       |                                |                                 |                           |  |  |
| 5         | APPLIANCE 5   |               |      |       |                       |                                |                                 |                           |  |  |
| 6         | APPLIANCE 6   |               |      |       |                       |                                |                                 |                           |  |  |
| 7         | APPLIANCE 7   |               |      |       |                       |                                |                                 |                           |  |  |
| 8         | APPLIANCE 8   |               |      |       |                       |                                |                                 |                           |  |  |
| 9         | APPLIANCE 9   |               |      |       |                       |                                |                                 |                           |  |  |
| 10        | APPLIANCE 10  |               |      |       |                       |                                |                                 |                           |  |  |

**Component IT Infra Supporting Software**

| Component | Operating System (OS) |                      |      |       |         |         |                   |  |
|-----------|-----------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | OS Model 1            |                      |      |       |         |         |                   |  |
| 2         | OS Model 2            |                      |      |       |         |         |                   |  |
| 3         | OS Model 3            |                      |      |       |         |         |                   |  |
| 4         | OS Model 4            |                      |      |       |         |         |                   |  |

| Component | Application server software (ASS) |                      |      |       |         |         |                   |  |
|-----------|-----------------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                     | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | ASS Model 1                       |                      |      |       |         |         |                   |  |
| 2         | ASS Model 2                       |                      |      |       |         |         |                   |  |
| 3         | ASS Model 3                       |                      |      |       |         |         |                   |  |
| 4         | ASS Model 4                       |                      |      |       |         |         |                   |  |

| Component | Web Server software (WSS) |                      |      |       |         |         |                   |  |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | WSS Model 1               |                      |      |       |         |         |                   |  |
| 2         | WSS Model 2               |                      |      |       |         |         |                   |  |
| 3         | WSS Model 3               |                      |      |       |         |         |                   |  |
| 4         | WSS Model 4               |                      |      |       |         |         |                   |  |

| Component | Backup Software |                      |      |       |         |         |                   |  |
|-----------|-----------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | BS Model 1      |                      |      |       |         |         |                   |  |
| 2         | BS Model 2      |                      |      |       |         |         |                   |  |
| 3         | BS Model 3      |                      |      |       |         |         |                   |  |
| 4         | BS Model 4      |                      |      |       |         |         |                   |  |

| Component | Virtualization/Containerization/HCI |                      |      |       |         |         |                   |  |
|-----------|-------------------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | VCH Model 1                         |                      |      |       |         |         |                   |  |
| 2         | VCH Model 2                         |                      |      |       |         |         |                   |  |
| 3         | VCH Model 3                         |                      |      |       |         |         |                   |  |
| 4         | VCH Model 4                         |                      |      |       |         |         |                   |  |

| Component | Database      |                      |      |       |         |         |                   |  |
|-----------|---------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | DB Model 1    |                      |      |       |         |         |                   |  |
| 2         | DB Model 2    |                      |      |       |         |         |                   |  |
| 3         | DB Model 3    |                      |      |       |         |         |                   |  |
| 4         | DB Model 4    |                      |      |       |         |         |                   |  |

| DC    |  |  |                   |                |               |                      |                    |               |   |   |
|-------|--|--|-------------------|----------------|---------------|----------------------|--------------------|---------------|---|---|
| S.No. | Server Reference (refer sheet Hardware BoQ ) | Software BoQ Reference (refer sheet Software BoQ ) | Zone (Web/App/Db) | vCores:P Cores | vCores per VM | vRAM (in GB ) per VM | HDD per VM (in GB) | Number of VMs | Storage Reference (refer sheet Hardware BoQ ) | Alloted Physical Storage (Usable) in GB |
| 1     |  |  |                   |                |               |                      |                    |               |   |   |
| 2     |  |  |                   |                |               |                      |                    |               |   |   |
| 3     |  |  |                   |                |               |                      |                    |               |   |   |
| 4     |  |  |                   |                |               |                      |                    |               |   |   |
| 5     |  |  |                   |                |               |                      |                    |               |   |   |
| 6     |  |  |                   |                |               |                      |                    |               |   |   |
| 7     |  |  |                   |                |               |                      |                    |               |   |   |
| 8     |  |  |                   |                |               |                      |                    |               |   |   |
| 9     |  |  |                   |                |               |                      |                    |               |   |   |
| 10    |  |  |                   |                |               |                      |                    |               |   |   |
| 11    |  |  |                   |                |               |                      |                    |               |   |   |
| 12    |  |  |                   |                |               |                      |                    |               |   |   |
| 13    |  |  |                   |                |               |                      |                    |               |   |   |
| 14    |  |  |                   |                |               |                      |                    |               |   |   |
| 15    |  |  |                   |                |               |                      |                    |               |   |   |
| 16    |  |  |                   |                |               |                      |                    |               |   |   |
| 17    |  |  |                   |                |               |                      |                    |               |   |   |
| 18    |  |  |                   |                |               |                      |                    |               |   |   |
| 19    |  |  |                   |                |               |                      |                    |               |   |   |
| 20    |  |  |                   |                |               |                      |                    |               |   |   |
| 21    |  |  |                   |                |               |                      |                    |               |   |   |
| 22    |  |  |                   |                |               |                      |                    |               |   |   |
| 23    |  |  |                   |                |               |                      |                    |               |   |   |
| 24    |  |  |                   |                |               |                      |                    |               |   |   |
| 25    |  |  |                   |                |               |                      |                    |               |   |   |
| 26    |  |  |                   |                |               |                      |                    |               |   |   |
| 27    |  |  |                   |                |               |                      |                    |               |   |   |
| 28    |  |  |                   |                |               |                      |                    |               |   |   |

| DR    |  |  |                   |                |               |                      |                    |               |   |   |
|-------|--|--|-------------------|----------------|---------------|----------------------|--------------------|---------------|---|---|
| S.No. | Server Reference (refer sheet Hardware BoQ ) | Software BoQ Reference (refer sheet Software BoQ ) | Zone (Web/App/Db) | vCores:P Cores | vCores per VM | vRAM (in GB ) per VM | HDD per VM (in GB) | Number of VMs | Storage Reference (refer sheet Hardware BoQ ) | Alloted Physical Storage (Usable) in GB |
| 1     |  |  |                   |                |               |                      |                    |               |   |   |
| 2     |  |  |                   |                |               |                      |                    |               |   |   |
| 3     |  |  |                   |                |               |                      |                    |               |   |   |
| 4     |  |  |                   |                |               |                      |                    |               |   |   |
| 5     |  |  |                   |                |               |                      |                    |               |   |   |
| 6     |  |  |                   |                |               |                      |                    |               |   |   |
| 7     |  |  |                   |                |               |                      |                    |               |   |   |
| 8     |  |  |                   |                |               |                      |                    |               |   |   |
| 9     |  |  |                   |                |               |                      |                    |               |   |   |
| 10    |  |  |                   |                |               |                      |                    |               |   |   |
| 11    |  |  |                   |                |               |                      |                    |               |   |   |
| 12    |  |  |                   |                |               |                      |                    |               |   |   |
| 13    |  |  |                   |                |               |                      |                    |               |   |   |
| 14    |  |  |                   |                |               |                      |                    |               |   |   |
| 15    |  |  |                   |                |               |                      |                    |               |   |   |
| 16    |  |  |                   |                |               |                      |                    |               |   |   |
| 17    |  |  |                   |                |               |                      |                    |               |   |   |
| 18    |  |  |                   |                |               |                      |                    |               |   |   |
| 19    |  |  |                   |                |               |                      |                    |               |   |   |
| 20    |  |  |                   |                |               |                      |                    |               |   |   |
| 21    |  |  |                   |                |               |                      |                    |               |   |   |
| 22    |  |  |                   |                |               |                      |                    |               |   |   |

|    |  |  |  |  |  |  |  |  |  |  |
|----|--|--|--|--|--|--|--|--|--|--|
| 23 |  |  |  |  |  |  |  |  |  |  |
| 24 |  |  |  |  |  |  |  |  |  |  |
| 25 |  |  |  |  |  |  |  |  |  |  |
| 26 |  |  |  |  |  |  |  |  |  |  |
| 27 |  |  |  |  |  |  |  |  |  |  |
| 28 |  |  |  |  |  |  |  |  |  |  |

| Non-production |  |  |                   |                |               |                      |                    |               |   |   |
|----------------|--|--|-------------------|----------------|---------------|----------------------|--------------------|---------------|---|---|
| S.No.          | Server Reference (refer sheet Hardware BoQ ) | Software BoQ Reference (refer sheet Software BoQ ) | Zone (Web/App/Db) | vCores:P Cores | vCores per VM | vRAM (in GB ) per VM | HDD per VM (in GB) | Number of VMs | Storage Reference (refer sheet Hardware BoQ ) | Alloted Physical Storage (Usable) in GB |
| 1              |  |  |                   |                |               |                      |                    |               |   |   |
| 2              |  |  |                   |                |               |                      |                    |               |   |   |
| 3              |  |  |                   |                |               |                      |                    |               |   |   |
| 4              |  |  |                   |                |               |                      |                    |               |   |   |
| 5              |  |  |                   |                |               |                      |                    |               |   |   |
| 6              |  |  |                   |                |               |                      |                    |               |   |   |
| 7              |  |  |                   |                |               |                      |                    |               |   |   |
| 8              |  |  |                   |                |               |                      |                    |               |   |   |
| 9              |  |  |                   |                |               |                      |                    |               |   |   |
| 10             |  |  |                   |                |               |                      |                    |               |   |   |
| 11             |  |  |                   |                |               |                      |                    |               |   |   |
| 12             |  |  |                   |                |               |                      |                    |               |   |   |
| 13             |  |  |                   |                |               |                      |                    |               |   |   |
| 14             |  |  |                   |                |               |                      |                    |               |   |   |
| 15             |  |  |                   |                |               |                      |                    |               |   |   |
| 16             |  |  |                   |                |               |                      |                    |               |   |   |
| 17             |  |  |                   |                |               |                      |                    |               |   |   |
| 18             |  |  |                   |                |               |                      |                    |               |   |   |
| 19             |  |  |                   |                |               |                      |                    |               |   |   |
| 20             |  |  |                   |                |               |                      |                    |               |   |   |
| 21             |  |  |                   |                |               |                      |                    |               |   |   |
| 22             |  |  |                   |                |               |                      |                    |               |   |   |
| 23             |  |  |                   |                |               |                      |                    |               |   |   |
| 24             |  |  |                   |                |               |                      |                    |               |   |   |
| 25             |  |  |                   |                |               |                      |                    |               |   |   |
| 26             |  |  |                   |                |               |                      |                    |               |   |   |
| 27             |  |  |                   |                |               |                      |                    |               |   |   |
| 28             |  |  |                   |                |               |                      |                    |               |   |   |



| DATA CENTER |                             |                      |      |       |         |         |                   |
|-------------|-----------------------------|----------------------|------|-------|---------|---------|-------------------|
| Component   | Application server software |                      |      |       |         |         |                   |
| S.No.       | BoQ Reference               | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1           | Appl SS Model 1             |                      |      |       |         |         |                   |
| 2           | Appl SS Model 2             |                      |      |       |         |         |                   |
| 3           | Appl SS Model 3             |                      |      |       |         |         |                   |
| 4           | Appl SS Model 4             |                      |      |       |         |         |                   |
| 5           | Appl SS Model 5             |                      |      |       |         |         |                   |

  

| Component | Web server software |                      |      |       |         |         |                   |
|-----------|---------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Web SS Model 1      |                      |      |       |         |         |                   |
| 2         | Web SS Model 2      |                      |      |       |         |         |                   |
| 3         | Web SS Model 3      |                      |      |       |         |         |                   |
| 4         | Web SS Model 4      |                      |      |       |         |         |                   |
| 5         | Web SS Model 5      |                      |      |       |         |         |                   |

  

| Component | Virtualization/HCI software |                      |      |       |         |         |                   |
|-----------|-----------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference               | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Virt SS Model 1             |                      |      |       |         |         |                   |
| 2         | Virt SS Model 2             |                      |      |       |         |         |                   |
| 3         | Virt SS Model 3             |                      |      |       |         |         |                   |
| 4         | Virt SS Model 4             |                      |      |       |         |         |                   |
| 5         | Virt SS Model 5             |                      |      |       |         |         |                   |

  

| Component | Operating system software |                      |      |       |         |         |                   |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Oper SS Model 1           |                      |      |       |         |         |                   |
| 2         | Oper SS Model 2           |                      |      |       |         |         |                   |
| 3         | Oper SS Model 3           |                      |      |       |         |         |                   |
| 4         | Oper SS Model 4           |                      |      |       |         |         |                   |
| 5         | Oper SS Model 5           |                      |      |       |         |         |                   |

  

| Component | Backup software |                      |      |       |         |         |                   |
|-----------|-----------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | BS Model 1      |                      |      |       |         |         |                   |
| 2         | BS Model 2      |                      |      |       |         |         |                   |
| 3         | BS Model 3      |                      |      |       |         |         |                   |
| 4         | BS Model 4      |                      |      |       |         |         |                   |
| 5         | BS Model 5      |                      |      |       |         |         |                   |

  

| Component | DRM (Digital Rights Management) |                      |      |       |         |         |                   |
|-----------|---------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | DRM Model 1                     |                      |      |       |         |         |                   |
| 2         | DRM Model 2                     |                      |      |       |         |         |                   |
| 3         | DRM Model 3                     |                      |      |       |         |         |                   |
| 4         | DRM Model 4                     |                      |      |       |         |         |                   |

  

| Component | Centralised Key Management |                      |      |       |         |         |                   |
|-----------|----------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference              | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | CKM Model 1                |                      |      |       |         |         |                   |
| 2         | CKM Model 2                |                      |      |       |         |         |                   |
| 3         | CKM Model 3                |                      |      |       |         |         |                   |
| 4         | CKM Model 4                |                      |      |       |         |         |                   |

  

| Component | Certificate Lifecycle Management |                      |      |       |         |         |                   |
|-----------|----------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                    | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | CLM Model 1                      |                      |      |       |         |         |                   |

|   |             |  |  |  |  |  |  |
|---|-------------|--|--|--|--|--|--|
| 2 | CLM Model 2 |  |  |  |  |  |  |
| 3 | CLM Model 3 |  |  |  |  |  |  |
| 4 | CLM Model 4 |  |  |  |  |  |  |

| Component | S-BOM & C-BOM       |                      |      |       |         |         |                   |
|-----------|---------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | SBOM & CBOM Model 1 |                      |      |       |         |         |                   |
| 2         | SBOM & CBOM Model 2 |                      |      |       |         |         |                   |
| 3         | SBOM & CBOM Model 3 |                      |      |       |         |         |                   |
| 4         | SBOM & CBOM Model 4 |                      |      |       |         |         |                   |

| Component | DAM (Database Activity Monitoring) |                      |      |       |         |         |                   |
|-----------|------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                      | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | DAM Model 1                        |                      |      |       |         |         |                   |
| 2         | DAM Model 2                        |                      |      |       |         |         |                   |
| 3         | DAM Model 3                        |                      |      |       |         |         |                   |
| 4         | DAM Model 4                        |                      |      |       |         |         |                   |

| Component | Mobile SDK (Software Development Kit) |                      |      |       |         |         |                   |
|-----------|---------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Mobile SDK Model 1                    |                      |      |       |         |         |                   |
| 2         | Mobile SDK Model 2                    |                      |      |       |         |         |                   |
| 3         | Mobile SDK Model 3                    |                      |      |       |         |         |                   |
| 4         | Mobile SDK Model 4                    |                      |      |       |         |         |                   |

| Component | IDAM (Identity and Access Management) |                      |      |       |         |         |                   |
|-----------|---------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | IDAM Model 1                          |                      |      |       |         |         |                   |
| 2         | IDAM Model 2                          |                      |      |       |         |         |                   |
| 3         | IDAM Model 3                          |                      |      |       |         |         |                   |
| 4         | IDAM Model 4                          |                      |      |       |         |         |                   |

| Component | IT GRC (Governance, Risk & Compliance) |                      |      |       |         |         |                   |
|-----------|--|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                          | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | ITGRC Model 1                          |                      |      |       |         |         |                   |
| 2         | ITGRC Model 2                          |                      |      |       |         |         |                   |
| 3         | ITGRC Model 3                          |                      |      |       |         |         |                   |
| 4         | ITGRC Model 4                          |                      |      |       |         |         |                   |

| Component | Multi-Factor Authenticaon |                      |      |       |         |         |                   |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | MFA Model 1               |                      |      |       |         |         |                   |
| 2         | MFA Model 2               |                      |      |       |         |         |                   |
| 3         | MFA Model 3               |                      |      |       |         |         |                   |
| 4         | MFA Model 4               |                      |      |       |         |         |                   |

| Component | PIM (Privileged Identity Management) |                      |      |       |         |         |                   |
|-----------|--------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                        | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | PIM Model 1                          |                      |      |       |         |         |                   |
| 2         | PIM Model 2                          |                      |      |       |         |         |                   |
| 3         | PIM Model 3                          |                      |      |       |         |         |                   |
| 4         | PIM Model 4                          |                      |      |       |         |         |                   |

| DISASTER RECOVERY CENTER |                             |                      |      |       |         |         |                   |
|--------------------------|-----------------------------|----------------------|------|-------|---------|---------|-------------------|
| Component                | Application server software |                      |      |       |         |         |                   |
| S.No.                    | BoQ Reference               | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1                        | Appl SS Model 1             |                      |      |       |         |         |                   |
| 2                        | Appl SS Model 2             |                      |      |       |         |         |                   |
| 3                        | Appl SS Model 3             |                      |      |       |         |         |                   |
| 4                        | Appl SS Model 4             |                      |      |       |         |         |                   |
| 5                        | Appl SS Model 5             |                      |      |       |         |         |                   |

| Component | Web server software |                      |      |       |         |         |                   |
|-----------|---------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Web SS Model 1      |                      |      |       |         |         |                   |
| 2         | Web SS Model 2      |                      |      |       |         |         |                   |
| 3         | Web SS Model 3      |                      |      |       |         |         |                   |
| 4         | Web SS Model 4      |                      |      |       |         |         |                   |
| 5         | Web SS Model 5      |                      |      |       |         |         |                   |

| Component | Virtualization/HCI software |                      |      |       |         |         |                   |
|-----------|-----------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference               | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Virt SS Model 1             |                      |      |       |         |         |                   |
| 2         | Virt SS Model 2             |                      |      |       |         |         |                   |
| 3         | Virt SS Model 3             |                      |      |       |         |         |                   |
| 4         | Virt SS Model 4             |                      |      |       |         |         |                   |
| 5         | Virt SS Model 5             |                      |      |       |         |         |                   |

| Component | Operating system software |                      |      |       |         |         |                   |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Oper SS Model 1           |                      |      |       |         |         |                   |
| 2         | Oper SS Model 2           |                      |      |       |         |         |                   |
| 3         | Oper SS Model 3           |                      |      |       |         |         |                   |
| 4         | Oper SS Model 4           |                      |      |       |         |         |                   |
| 5         | Oper SS Model 5           |                      |      |       |         |         |                   |

| Component | Backup software |                      |      |       |         |         |                   |
|-----------|-----------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | BS Model 1      |                      |      |       |         |         |                   |
| 2         | BS Model 2      |                      |      |       |         |         |                   |
| 3         | BS Model 3      |                      |      |       |         |         |                   |
| 4         | BS Model 4      |                      |      |       |         |         |                   |
| 5         | BS Model 5      |                      |      |       |         |         |                   |

| Component | DRM (Digital Rights Management) |                      |      |       |         |         |                   |
|-----------|---------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | DRM Model 1                     |                      |      |       |         |         |                   |
| 2         | DRM Model 2                     |                      |      |       |         |         |                   |
| 3         | DRM Model 3                     |                      |      |       |         |         |                   |
| 4         | DRM Model 4                     |                      |      |       |         |         |                   |

| Component | Centralised Key Management |                      |      |       |         |         |                   |
|-----------|----------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference              | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | CKM Model 1                |                      |      |       |         |         |                   |
| 2         | CKM Model 2                |                      |      |       |         |         |                   |
| 3         | CKM Model 3                |                      |      |       |         |         |                   |

|   |             |  |  |  |  |  |  |
|---|-------------|--|--|--|--|--|--|
| 4 | CKM Model 4 |  |  |  |  |  |  |
|---|-------------|--|--|--|--|--|--|

| Component | Certificate Lifecycle Management |                      |      |       |         |         |                   |
|-----------|----------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                    | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | CLM Model 1                      |                      |      |       |         |         |                   |
| 2         | CLM Model 2                      |                      |      |       |         |         |                   |
| 3         | CLM Model 3                      |                      |      |       |         |         |                   |
| 4         | CLM Model 4                      |                      |      |       |         |         |                   |

| Component | S-BOM & C-BOM       |                      |      |       |         |         |                   |
|-----------|---------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | SBOM & CBOM Model 1 |                      |      |       |         |         |                   |
| 2         | SBOM & CBOM Model 2 |                      |      |       |         |         |                   |
| 3         | SBOM & CBOM Model 3 |                      |      |       |         |         |                   |
| 4         | SBOM & CBOM Model 4 |                      |      |       |         |         |                   |

| Component | DAM (Database Activity Monitoring) |                      |      |       |         |         |                   |
|-----------|------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                      | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | DAM Model 1                        |                      |      |       |         |         |                   |
| 2         | DAM Model 2                        |                      |      |       |         |         |                   |
| 3         | DAM Model 3                        |                      |      |       |         |         |                   |
| 4         | DAM Model 4                        |                      |      |       |         |         |                   |

| Component | Mobile SDK (Software Development Kit) |                      |      |       |         |         |                   |
|-----------|---------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Mobile SDK Model 1                    |                      |      |       |         |         |                   |
| 2         | Mobile SDK Model 2                    |                      |      |       |         |         |                   |
| 3         | Mobile SDK Model 3                    |                      |      |       |         |         |                   |
| 4         | Mobile SDK Model 4                    |                      |      |       |         |         |                   |

| Component | IDAM (Identity and Access Management) |                      |      |       |         |         |                   |
|-----------|---------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | IDAM Model 1                          |                      |      |       |         |         |                   |
| 2         | IDAM Model 2                          |                      |      |       |         |         |                   |
| 3         | IDAM Model 3                          |                      |      |       |         |         |                   |
| 4         | IDAM Model 4                          |                      |      |       |         |         |                   |

| Component | IT GRC (Governance, Risk & Compliance) |                      |      |       |         |         |                   |
|-----------|--|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                          | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | ITGRC Model 1                          |                      |      |       |         |         |                   |
| 2         | ITGRC Model 2                          |                      |      |       |         |         |                   |
| 3         | ITGRC Model 3                          |                      |      |       |         |         |                   |
| 4         | ITGRC Model 4                          |                      |      |       |         |         |                   |

| Component | Multi-Factor Authenticaon |                      |      |       |         |         |                   |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | MFA Model 1               |                      |      |       |         |         |                   |
| 2         | MFA Model 2               |                      |      |       |         |         |                   |
| 3         | MFA Model 3               |                      |      |       |         |         |                   |
| 4         | MFA Model 4               |                      |      |       |         |         |                   |

| Component | PIM (Privileged Identity Management) |                      |      |       |         |         |                   |
|-----------|--------------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                        | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | PIM Model 1                          |                      |      |       |         |         |                   |

|   |             |  |  |  |  |  |  |
|---|-------------|--|--|--|--|--|--|
| 2 | PIM Model 2 |  |  |  |  |  |  |
| 3 | PIM Model 3 |  |  |  |  |  |  |
| 4 | PIM Model 4 |  |  |  |  |  |  |

| NON-PRODUCTION |                             |                      |      |       |         |         |                   |
|----------------|-----------------------------|----------------------|------|-------|---------|---------|-------------------|
| Component      | Application server software |                      |      |       |         |         |                   |
| S.No.          | BoQ Reference               | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1              | Appl SS Model 1             |                      |      |       |         |         |                   |
| 2              | Appl SS Model 2             |                      |      |       |         |         |                   |
| 3              | Appl SS Model 3             |                      |      |       |         |         |                   |
| 4              | Appl SS Model 4             |                      |      |       |         |         |                   |
| 5              | Appl SS Model 5             |                      |      |       |         |         |                   |

| Component | Web server software |                      |      |       |         |         |                   |
|-----------|---------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Web SS Model 1      |                      |      |       |         |         |                   |
| 2         | Web SS Model 2      |                      |      |       |         |         |                   |
| 3         | Web SS Model 3      |                      |      |       |         |         |                   |
| 4         | Web SS Model 4      |                      |      |       |         |         |                   |
| 5         | Web SS Model 5      |                      |      |       |         |         |                   |

| Component | Virtualization/HCI software |                      |      |       |         |         |                   |
|-----------|-----------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference               | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Virt SS Model 1             |                      |      |       |         |         |                   |
| 2         | Virt SS Model 2             |                      |      |       |         |         |                   |
| 3         | Virt SS Model 3             |                      |      |       |         |         |                   |
| 4         | Virt SS Model 4             |                      |      |       |         |         |                   |
| 5         | Virt SS Model 5             |                      |      |       |         |         |                   |

| Component | Operating system software |                      |      |       |         |         |                   |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | Oper SS Model 1           |                      |      |       |         |         |                   |
| 2         | Oper SS Model 2           |                      |      |       |         |         |                   |
| 3         | Oper SS Model 3           |                      |      |       |         |         |                   |
| 4         | Oper SS Model 4           |                      |      |       |         |         |                   |
| 5         | Oper SS Model 5           |                      |      |       |         |         |                   |

| Component | Backup software |                      |      |       |         |         |                   |
|-----------|-----------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | BS Model 1      |                      |      |       |         |         |                   |
| 2         | BS Model 2      |                      |      |       |         |         |                   |
| 3         | BS Model 3      |                      |      |       |         |         |                   |
| 4         | BS Model 4      |                      |      |       |         |         |                   |
| 5         | BS Model 5      |                      |      |       |         |         |                   |

| Component | DRM (Digital Rights Management) |                      |      |       |         |         |                   |
|-----------|---------------------------------|----------------------|------|-------|---------|---------|-------------------|
| S.No.     | BoQ Reference                   | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |
| 1         | DRM Model 1                     |                      |      |       |         |         |                   |
| 2         | DRM Model 2                     |                      |      |       |         |         |                   |
| 3         | DRM Model 3                     |                      |      |       |         |         |                   |
| 4         | DRM Model 4                     |                      |      |       |         |         |                   |

| Component | Centralised Key Management |                      |      |       |         |         |                   |  |
|-----------|----------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference              | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | CKM Model 1                |                      |      |       |         |         |                   |  |
| 2         | CKM Model 2                |                      |      |       |         |         |                   |  |
| 3         | CKM Model 3                |                      |      |       |         |         |                   |  |
| 4         | CKM Model 4                |                      |      |       |         |         |                   |  |

| Component | Certificate Lifecycle Management |                      |      |       |         |         |                   |  |
|-----------|----------------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                    | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | CLM Model 1                      |                      |      |       |         |         |                   |  |
| 2         | CLM Model 2                      |                      |      |       |         |         |                   |  |
| 3         | CLM Model 3                      |                      |      |       |         |         |                   |  |
| 4         | CLM Model 4                      |                      |      |       |         |         |                   |  |

| Component | S-BOM & C-BOM       |                      |      |       |         |         |                   |  |
|-----------|---------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference       | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | SBOM & CBOM Model 1 |                      |      |       |         |         |                   |  |
| 2         | SBOM & CBOM Model 2 |                      |      |       |         |         |                   |  |
| 3         | SBOM & CBOM Model 3 |                      |      |       |         |         |                   |  |
| 4         | SBOM & CBOM Model 4 |                      |      |       |         |         |                   |  |

| Component | DAM (Database Activity Monitoring) |                      |      |       |         |         |                   |  |
|-----------|------------------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                      | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | DAM Model 1                        |                      |      |       |         |         |                   |  |
| 2         | DAM Model 2                        |                      |      |       |         |         |                   |  |
| 3         | DAM Model 3                        |                      |      |       |         |         |                   |  |
| 4         | DAM Model 4                        |                      |      |       |         |         |                   |  |

| Component | Mobile SDK (Software Development Kit) |                      |      |       |         |         |                   |  |
|-----------|---------------------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | Mobile SDK Model 1                    |                      |      |       |         |         |                   |  |
| 2         | Mobile SDK Model 2                    |                      |      |       |         |         |                   |  |
| 3         | Mobile SDK Model 3                    |                      |      |       |         |         |                   |  |
| 4         | Mobile SDK Model 4                    |                      |      |       |         |         |                   |  |

| Component | IDAM (Identity and Access Management) |                      |      |       |         |         |                   |  |
|-----------|---------------------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                         | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | IDAM Model 1                          |                      |      |       |         |         |                   |  |
| 2         | IDAM Model 2                          |                      |      |       |         |         |                   |  |
| 3         | IDAM Model 3                          |                      |      |       |         |         |                   |  |
| 4         | IDAM Model 4                          |                      |      |       |         |         |                   |  |

| Component | IT GRC (Governance, Risk & Compliance) |                      |      |       |         |         |                   |  |
|-----------|--|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                          | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | ITGRC Model 1                          |                      |      |       |         |         |                   |  |
| 2         | ITGRC Model 2                          |                      |      |       |         |         |                   |  |
| 3         | ITGRC Model 3                          |                      |      |       |         |         |                   |  |
| 4         | ITGRC Model 4                          |                      |      |       |         |         |                   |  |

| Component | Multi-Factor Authenticaon |                      |      |       |         |         |                   |  |
|-----------|---------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference             | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | MFA Model 1               |                      |      |       |         |         |                   |  |
| 2         | MFA Model 2               |                      |      |       |         |         |                   |  |
| 3         | MFA Model 3               |                      |      |       |         |         |                   |  |
| 4         | MFA Model 4               |                      |      |       |         |         |                   |  |

| Component | PIM (Privileged Identity Management) |                      |      |       |         |         |                   |  |
|-----------|--------------------------------------|----------------------|------|-------|---------|---------|-------------------|--|
| S.No.     | BoQ Reference                        | Qty of proposed Item | Make | Model | Version | Edition | Licensing Metrics |  |
| 1         | PIM Model 1                          |                      |      |       |         |         |                   |  |
| 2         | PIM Model 2                          |                      |      |       |         |         |                   |  |
| 3         | PIM Model 3                          |                      |      |       |         |         |                   |  |
| 4         | PIM Model 4                          |                      |      |       |         |         |                   |  |

| FM Support (Total across locations) |                            |                           |                            |  |
|-------------------------------------|----------------------------|---------------------------|----------------------------|--|
| BoQ Reference                       | Shift 1 (Qty of Resources) | Shift 2(Qty of Resources) | Shift 3 (Qty of Resources) | Name of the proposed Resources   |
| Project Manager                     |                            |                           |                            |  |
| Deputy Coordinator 1                |                            |                           |                            |  |
| Deputy Coordinator 2                |                            |                           |                            |  |
| L1                                  |                            |                           |                            | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| L2                                  |                            |                           |                            | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| L3                                  |                            |                           |                            | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| L0 helpdesk                         |                            |                           |                            | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |



|                           |  |  |  |  |
|---------------------------|--|--|--|--|
| Any other, please specify |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
|---------------------------|--|--|--|--|

| Implementation Team   |                            |                           |                            |  |
|---|----------------------------|---------------------------|----------------------------|--|
| BoQ Reference   | Shift 1 (Qty of Resources) | Shift 2(Qty of Resources) | Shift 3 (Qty of Resources) | Name of the proposed Resources   |
| Project Manager   |                            |                           |                            |  |
| Deputy Coordinator 1  |                            |                           |                            |  |
| Deputy Coordinator 2  |                            |                           |                            |  |
| Any other, please specify   |                            |                           |                            | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| DRM (Digital Rights Management)                                   |                            |                           |                            |  |
| Project Manager   |                            |                           |                            |  |
| Implementation Team   |                            |                           |                            |  |
| Testing Team  |                            |                           |                            |  |
| Bidder resources mapped to the solution during the implementation |                            |                           |                            |  |
| Any other, please specify   |                            |                           |                            | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| Centralised Key Management  |                            |                           |                            |  |
| Project Manager   |                            |                           |                            |  |
| Implementation Team   |                            |                           |                            |  |
| Testing Team  |                            |                           |                            |  |
| Bidder resources mapped to the solution during the implementation |                            |                           |                            |  |

|   |  |  |  |  |
|---|--|--|--|--|
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>Certificate Lifecycle Management</b>                           |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |
| Bidder resources mapped to the solution during the implementation |  |  |  |  |
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>S-BOM &amp; C-BOM (Software and Code Bill of Materials)</b>    |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |
| Bidder resources mapped to the solution during the implementation |  |  |  |  |
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>DAM (Database Activity Monitoring)</b>                         |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |
| Bidder resources mapped to the solution during the implementation |  |  |  |  |

|   |  |  |  |  |
|---|--|--|--|--|
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>Mobile SDK (Software Development Kit)</b>                      |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |
| Bidder resources mapped to the solution during the implementation |  |  |  |  |
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>IDAM (Identity and Access Management)</b>                      |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |
| Bidder resources mapped to the solution during the implementation |  |  |  |  |
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>IT GRC (Governance, Risk &amp; Compliance)</b>                 |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |

|   |  |  |  |  |
|---|--|--|--|--|
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>Multi-Factor Authenticator</b>                                 |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |
| Bidder resources mapped to the solution during the implementation |  |  |  |  |
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |
| <b>PIM (Privileged Identity Management)</b>                       |  |  |  |  |
| Project Manager   |  |  |  |  |
| Implementation Team   |  |  |  |  |
| Testing Team  |  |  |  |  |
| Bidder resources mapped to the solution during the implementation |  |  |  |  |
| Any other, please specify   |  |  |  | a. <Name of the proposed resource><br>b. <Name of the proposed resource><br>c. <Name of the proposed resource><br>d. <Name of the proposed resource><br>e. <Name of the proposed resource><br>f. <Name of the proposed resource><br>g. <Name of the proposed resource><br>Add the name based on the Total proposed resources |

| OTHER ITEMS   |                |
|---------------|----------------|
| BoQ Reference | Name & Details |
| Escrow Agency |                |
|               |                |