

S. No	Solution Name	Maximum Mark Allocated	Maximum Mark Obtained	Respective Solution Compliance (%)
1	Anti-DDoS			
2	SSL Orchestrator Tool and Packet Broker			
3	DNS Protection			
4	Web Gateway			
5	Zero-Day Attack Protection for Endpoint and Network			
6	ZTNA			
7	DLP			
8	Information/ Digital Rights Management			
9	Database Activity Monitoring			
10	Mobile SDK			
11	HIPS			
12	WAF			
13	Centralised Key Management			
14	Certificate Lifecycle Management			
15	IDAM			
16	MFA			
17	PIM			
18	DNS Security			
19	CASB			
20	SBOM, CBOM, AI-BOM and QBOM			
21	AI Security			
GRAND TOTAL		0	0	

Instructions

Maximum Marks	Compliance (S/C)	Maximum Mark
10	S (Standard):	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.
3	C (Customization):	• Requirements marked as C (Customization) go beyond what is available or possible through standard product configuration. - Customization involves: • Development of custom code • Creation of new functionalities or interfaces • Modifications that may impact upgrade paths or require specific deployment and testing cycles • User interface enhancements or custom-built screens • 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	In case bidder has provided the response which is neither "S" or "C". The requirement shall be considered as "No"or "N", the bid shall be liable for rejection
5	All the above mentioned features should be available form the day 1.

Anti DDoS					
S. No.	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	System should be Stateless appliances in DC and DR, It should be sized on clean traffic throughput irrespective of mitigation. System should support unlimited number of concurrent sessions.	10	Select	0	
2	System should have 5 Gbps of clean/legitimate throughput which can scale upto 10 Gbps on the same H/w. System should support more then 20 MPPS. System should be factored on clean/legitimate license throughput.	10	Select	0	
3	System should have 8x10 G ports with fail open support without any external fail open kit. All the interfaces including fiber should support fail open.	10			
4	Latency <=80 microseconds	10	Select	0	
5	Device should be rack mountable in standard 42 U Rack and all the necessary equipment required for device mounting on racks should be included from day 1.	10	Select	0	
6	Proposed product/solution should be stateless Technology not having any kind of state limitation e.g. TCP connections, unlimited attack concurrent sessions	10	Select	0	
7	Detect and Mitigate both inbound and outbound traffic	10	Select	0	
8	Work in fail open mode in all the ports and should support software and hardware bypass capability	10	Select	0	
9	Protect from multiple attack vectors on different layers at the same time with combination OS, Network, Application, and Server side attacks	10	Select	0	
10	Detect and mitigate IPV4 & IPv6 Attacks	10	Select	0	
11	Detect and block the traffic originated from any specific using Geo location based filtering	10	Select	0	
12	Inbuilt mechanism to inspect traffic with external threat feed. System should support minimum 2 million IoC's for both inbound and outbound blocking.	10	Select	0	
13	Detect and block traffic originated from source IP address(IPV6 AND IPV4) from TOR network	10	Select	0	
14	Support Symmetric and Asymmetric Traffic flows	10	Select	0	
15	Support integration of external Threat Intelligence Platform (TIP) on STIX / TAXI 2.0	10	Select	0	
16	Detect and block ICMP, FTP Floods, Botnets, DNS Floods including, A, MX, PTR, AAAA, Text, SOA, NAPTR, SRV etc.	10	Select	0	
17	Detect and Mitigate attacks at Layer 3 to Layer 7	10	Select	0	
18	Protect from TCP Out-Of-State attacks	10	Select	0	
19	The proposed DDoS device to transparently forward VLAN-tagged frames and encapsulated control protocols (like L2TP and GRE) across network segments. This ensures VLAN separation, VPN tunnels, and essential control traffic remain functional even while the device monitors or filters traffic for security purposes.	10	Select	0	
20	Detect misuse of application protocols in the network like HTTP/POP3/STP/SIP/SMTP/FTP	10	Select	0	
21	Mitigation mechanism to protecting against zero-day DoS and DDoS attacks without manual intervention. Automatic Real time signature generation	10	Select	0	
22	Protect against SSL/TLS-encrypted DoS and DDoS threats both at the SSL /TLS layer and HTTPS layer System should Protect against SSL/TLS-encrypted Attacks. Indicative HTTPS Protection method: *First/Initial Request Mitigation on Suspect Sources *Keyless Mitigation or Keyless inspection *First/Initial Request Mitigation on All Sources *Selective Full Inspection	10	Select	0	
23	Block invalid packets (including checks for Malformed IP Header, Incomplete Fragment, Bad IP Checksum, Duplicate Fragment, Fragment Too Long, Short Packet, Short TCP Packet, Short UDP Packet, Short ICMP Packet, Bad TCP / UDP Checksum, Invalid TCP Flags, Invalid ACK Number) and provide statistics for the packets dropped. Solution should also support packet Anomaly Protection	10	Select	0	
24	Support deployment on a "logical link bundle" interfaces, In-Line, Out-of-Path deployments modes.	10	Select	0	
25	Support comprehensive countermeasure to protect against zero-day attack, Challenge - Response Mechanism, and which should be able to Detect and protect attacks in real time.	10	Select	0	

26	Detect and protect from unknown Network & application layer DDOS attacks . System should support Behavioural based predictive DDoS protection. The proposed Appliance should support below Security Protection Profiles: 1. Behavioral based DoS/DDoS protection.. 2. DNS Protections.. 3. SYN-Flood Protection. 4. Configurable traffic filtering 5. Out-of-State Protection. 6. Anti-Scanning/"Detect and mitigate network reconnaissance and scanning activities" 7. Connection Limit. 8. Signature based Protection. 9. HTTPS Protection. 10. Web DDoS Protection.	10	Select	0	
27	Support suspension/dynamic suspension of traffic from offending source based on a signature detection and attack countermeasures	10	Select	0	
28	Support the dropping of idle TCP sessions if client does not send a data in defined time and should dynamically blacklist the offending sources	10	Select	0	
29	Ability to limit the number of connections depending on source or range	10	Select	0	
30	Allow Network Security policies to be changed while the policy is in active blocking mode and should not affect running network protection.	10	Select	0	
31	Should have countermeasures & challenge response based approach for immediate mitigation of flood attacks—protecting against unknown DDoS attacks without manual intervention. The system should not depend on only signatures for mitigation of DDOS attacks.	10	Select	0	
32	Able to detect and block SYN Flood attacks and should support different mechanism a) SYN Protection - TCP Authentication b) SYN Protection - Out of Sequence Authentication c) SYN Protection - TCP Reset	10	Select	0	
33	Able to detect and block HTTP GET Flood and should support following mechanism to avoid False Positive prevention (or equivalent): a)TCP Authentication b) HTTP REGEX payload and header c) Malformed HTTP Header d) Behavioral based HTTP	10	Select	0	
34	Support minimum 20 K SSL CPS on TLS 1.3 with selective decryption and TLS fingerprinting. Also System should have ability to scale SSL CPS capacity via external SSL appliance retaining proposed DDoS appliance (CPS: Connections Per Second)	10	Select	0	
35	Protect from Brute Force/reflection & amplification attacks or equivalent	10	Select	0	
36	Detect from Known DDoS attack Tools without any performance impact	10	Select	0	
37	Console Access should allow configuration via standard up to date web browsers	10	Select	0	
38	Provide protection for known attack tools that attack vulnerabilities in the SSL layer itself or separate SSL offloading device	10	Select	0	
39	Support following environments: Symmetric, Asymmetric	10	Select	0	
40	Support horizontal and vertical port scanning Behavioral protection	10	Select	0	
41	Built-in hardware bypass for all interface types for copper and fiber interfaces.	10	Select	0	
42	Detect and Mitigate different categories of Network Attacks viz . Volume based, Protocol, Application attacks etc.	10	Select	0	
43	Should detect SSL encrypted attacks at Key size 1K & 2K	10	Select	0	
44	Able to detect and protect from Zero-Day Network DDoS/DDoS flood attacks on the basis of behavioral DDoS attacks/challenge response mechanism or by an automatically created signature / countermeasure within a minute and must be mentioned in data sheet. The proposed device should also support inbuilt Signatures apart from custom Signatures from Day 1.	10	Select	0	
45	Identify malicious SSL traffic based on behavior analysis and to decrypt only malicious identified traffic instead of inspecting entire traffic to reduce the latency.	10	Select	0	
46	Cloud signaling to signal to upstream ISPs who is providing anti-DDoS cloud service clean pipe for very large DDoS attack mitigation. The signaling should be native / REST API. No data should be required to be routed to any third party cloud provider. No Data/information shall leave Indian Sub-continent at any point and shall adhere to MEITY, RBI and GOI Guidelines at all time during the contract period.	10	Select	0	
47	DDoS Appliance must not have any limitations in handling the number of concurrent session for DDoS attack traffic - Knowing nature of solution and should be clearly mentioned in public facing datasheet.	10	Select	0	
48	Device should have High performance architecture to ensure that attack mitigation does not affect normal traffic processing.	10	Select	0	
49	Quoted OEM should have Global Technical Assistance (TAC) support in India	10	Select	0	

50	The Solution should be proposed with centralized management for all the proposed DDoS protection Appliance at both DC & DR	10	Select	0	
51	Should have Role/User Based Access Control and reporting functionality.	10	Select	0	
52	Centralized management should have mechanism to update policies, configuration and applications of the DDoS Protection appliance centrally.	10	Select	0	
53	In inline mode system must not modify MAC or IP addresses of passed frames	10	Select	0	
54	The Device must have an updated IP reputation feed that describes suspicious traffic, Blacklisted IPs, botnets, Phishing. It should be updated as and when made available by OEM to block and protect network against active attackers.	10	Select	0	
55	The Proposed Anti-DDoS solution should be integrated with OEM Threat intelligence feed or from reputed Threat intelligence feed specific to DDoS Attacks & prevention without any additional cost to the bank for the duration of the contract.	10	Select	0	
56	The proposed DDOS protection should provide user customizable/ user definable signature/countermeasures	10	Select	0	
57	System should be able to provide Challenge action apply to suspicious/all source.	10	Select	0	
58	System DNS protection should employ challenge/response and rate limiting mechanism with TC bit set.	10	Select	0	
59	Real-time events correlation between Multi Vector Attacks viz. Volume based, Protocol, Application attacks etc.	10	Select	0	
60	Device should integrate with Banks SIEM engine seamlessly through syslog messages	10	Select	0	
61	System should mitigate all types of attack including known and unknown attacks	10	Select	0	
62	System should accurately follow attack vector changes without pcap analysis required or manual scripts	10	Select	0	
63	System should have out-of-path / on device SSL inspection	10	Select	0	
64	Proposed Anti-DDoS Solution should Protect against SSL based attacks.	10	Select	0	
65	All components of the solution should be capable of High Availability and the deployment should be enabled from Day 1	10	Select	0	
66	The proposed solution shall support detection and mitigation of DDoS attacks using configurable and adaptive traffic analysis techniques to identify abnormal or malicious network traffic while minimizing false positives.	10	Select	0	
67	The proposed solution shall support detection and mitigation of DNS-based denial-of-service attacks and other attacks targeting DNS services using signature-based, behavioral, query-response analysis, or equivalent techniques.	10	Select	0	
68	The proposed solution shall provide visibility into the characteristics, vectors, and protocols associated with detected DDoS attacks to support analysis, investigation, and response.	10	Select	0	
69	The proposed solution shall support analysis and/or classification of encrypted network traffic using behavioral, statistical, metadata-based, TLS/traffic-fingerprinting, or equivalent techniques to enhance detection of malicious activity, without mandating full decryption of encrypted payloads, where applicable.	10	Select	0	
70	The proposed solution shall support on-premises appliance-based, cloud-based/service-provider-hosted (scrubbing center), or hybrid architectures combining on-premises and cloud-based mitigation, as applicable to the Bank's deployment requirements.	10	Select	0	
71	The proposed solution shall support detection of known and emerging DDoS attacks using one or more analysis techniques, including signature-based, heuristic, behavioural, statistical, artificial intelligence, machine learning, or equivalent methods, where supported.	10	Select	0	
72	The proposed solution shall support configurable detection policies, profiles, and/or thresholds to improve the effectiveness of DDoS detection and mitigation in accordance with the Bank's operational requirements.	10	Select	0	
73	The proposed solution shall support PQC readiness and migration capability, including identification of quantum-vulnerable cryptographic algorithms and support for PQC-enabled or quantum-resistant cryptographic standards, wherever applicable to the solution.	10	Select	0	
A	DDoS Cloud Mitigation: ISP clean pipe mitigation				
74	Protection from all attacks like UDP Flooding, ICMP Flooding, Spoofed packet Flooding,SYN Floods, fragmented packet attacks, Ping od Death, Smurf, GET/POST floods, Zero Day DDoS etc.	10	Select	0	
75	Solution must support blocking of multiple IP's in one go by uploading csv, txt or any other file type on all the gateways being managed by the management server.	10	Select	0	
76	OEM should provide 24X7 Single Point of Contact(SPOC) details for any issue.	10	Select	0	
77	Anti-DDoS Solution should enable and provide features like null routing, sinkholing, scrubbing, IP masking, DNS name server protection from NXDomain attacks, with uptime SLA of 99.99%	10	Select	0	
Total		770		0	

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

SSL Orchestrator with Packet Broker (NETWORK VISIBILITY DEVICES or Network Packet Broker Solution)					
Sr.No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
PACKET BROKER					
A	SYSTEM				
1	The Solution must support backplane capacity of at least 2 Tbps throughput	10	Select	0	
2	The Solution must support optional clustering of at least 50 nodes in a single logical system with "manage-as-one" cluster-wide configuration capabilities.	10	Select	0	
3	The Solution must operate at full line-rate without packet loss.	10	Select	0	
4	The Solution must Operates at five different speeds — 1G, 10G, 25G, 40G, and 100G networks, Features 48 SFP28 ports that support 1G, 10G, and 25G	10	Select	0	
5	The Solution must support at least 48 ports of native 1G/10G/25G in 1 RU rackspace	10	Select	0	
6	The Solution must have additional Supports of eight QSFP28 ports that support 40G and 100G in 1 RU rack space which should be provisioned as and when required by bank	10	Select	0	
7	The solution must support port aggregation, mapping of input port to output port in a simple GUI without requiring CLI coding	10	Select	0	
8	The solution must support to configure all filtering capacities via GUI.	10	Select	0	
9	The solution must support jumbo frame packet.	10	Select	0	
10	Vendor-Neutral Hardware Specification: Rewrites hardware requirements away from an exact port layout and specific ASIC characteristics that match one particular OEM's product, and instead defines them in terms of outcome-based criteria — minimum port counts, required throughput, and rack space footprint. This opens the requirement to genuine competition from multiple qualified vendors while still guaranteeing the capacity and physical form-factor the deployment needs.	10	Select	0	
11	Packet Grooming: Adds a set of traffic-optimization capabilities beyond basic filtering and load balancing before packets reach security tools — including de-duplication of repeated packets, packet slicing (trimming packets to only the relevant portion, e.g., headers), stripping of encapsulation headers/tags (VLAN, MPLS, VXLAN, GRE, ERSPAN), payload masking of sensitive data, and generation of flow metadata. This reduces the bandwidth and processing load placed on downstream security tools while improving the relevance of what they actually inspect.	10	Select	0	
12	Secure Configuration Backup: Removes FTP as an allowed method for scheduled configuration backups, since it transmits data (including credentials) in plaintext, and mandates the use of secure alternatives only — SFTP, SCP, or FTPS. This closes off a common insecure-by-default configuration pathway and ensures backup data is protected in transit.	10	Select	0	
B	Hardware				
13	The Hardware must support fully redundant AC or DC power supplies.	10	Select	0	
14	The Hardware must support hot-swappable power supplies and fans, without the requirement for reboot during swapping.	10	Select	0	
15	The Hardware must support to fit into a standard 19 inch rack.	10	Select	0	
16	The Hardware must support front-to-back airflow for cooling.	10	Select	0	
17	The Hardware must support the following environmental specifications:				
17.1	Operating Temperature: 0C to 40C	10	Select	0	
17.2	Operating Relative Humidity: 5% to 95%, non-condensing	10	Select	0	
C	Port Support				
18	The Solution must support the flexibility to have Supports 1/10/25G and 40/100G port speeds, including fan-in and fan-out support., without additional license	10	Select	0	
19	The Solution must support flexible ingress/egress ports, where all ports can be user configured as either network or tool ports.	10	Select	0	
20	The Solution must support each port to be used at ingress and egress simultaneously.	10	Select	0	
21	The Solution must support software loopback port to loop the traffic internally for the advanced filtering	10	Select	0	
22	The solution must support port change status traps.	10	Select	0	
23	The solution must support to configure to transmit light or not per each port	10	Select	0	
24	The solution must support to assign IP address on each ingress port, and have an option to send periodic Gratuitous ARP Reply packets on the port for the configured IP.	10	Select	0	
D	Inline Features				
25	The Solution must support the integration with external bypass switch, must supports failsafe serial service chaining, parallel load balancing with spares, or combined topologies	10	Select	0	
26	The Inline solution must be separate bypass switch and Solution domains with different hardware's.	10	Select	0	

27	The external bypass solution must have high availability capability in order to enable resilient and HA architecture. E.g. active/active and active/standby	10	Select	0	
28	The Solution must support one-to-one, one-to-many, many-to-one, many-to-many inline configurations to better leverage the inline tools available	10	Select	0	
29	The Solution must support graphically configuration for intelligent and easy inline setup, without complex logic manipulation of traffic flow, CLI and filter rules setup.	10	Select	0	
30	The Solution must support bidirectional heartbeat that monitors inline tool health on both direction of traffic flows.	10	Select	0	
31	The Solution must support heartbeat pattern's MACs to flip (reverse source and destination MAC) on the reverse direction of traffic.	10	Select	0	
32	The Solution must support intelligent inline application setup and traffic load balancing and re-route between inline devices (e.g. connect with Firewall or IPS and inline SSL decryption/encryption).	10	Select	0	
33	The Solution must support N+1 and 1+1 inline tool redundancy for inline tools	10	Select	0	
34	The Solution must support HA active-active setup with the inline tools. (i.e. two Solution boxes work in active-active mode)	10	Select	0	
35	The HA failover among HA packet brokers must be within 1 second range	10	Select	0	
36	The Solution must support Link Fault Detection (LFD), this is to help to bring down the port pair when one of the port goes down.	10	Select	0	
37	The Solution must support to trigger the selected port(s) to go down on the same box or on the HA's opposite box when LFD enabled.	10	Select	0	
38	The Solution must support VLAN tag to the traffic comes from bypass switch(es)	10	Select	0	
39	The Solution must support VLAN translation in case of inline tools doesn't support QinQ tags	10	Select	0	
40	The Solution must support Inline Service Chaining and can support at least 5 sets of security tools in a single module	10	Select	0	
41	The Solution's Inline Service chaining function must support load balance traffic to different sets of tool farm.	10	Select	0	
42	The load balancing criteria should not be limited to hash based or traffic weight based with low and high watermark. (note : low/high watermark refers to min/max available tool to failover)	10	Select	0	
43	The Solution must support to mirror multiple copies of traffic to the passive tools which connected to the same Solution.	10	Select	0	
44	The Solution must support to selectively pass the traffic to certain tools, e.g. deny the traffic like multicast, broadcast and non - http (s) traffic.	10	Select	0	
E Management, monitoring and Security					
45	The solution must have intuitive GUI for management purpose.	10	Select	0	
46	The solution must support a serial console port, the tasks to be done on console port includes at least IP address changes/POST tests/Reset admin pass/shutdown systems/Reboot systems	10	Select	0	
47	The solution must support to configure everything on GUI instead of certain setup to defer to CLI configuration	10	Select	0	
48	The Solution must support role-based access (privilege) and must be able to be viewed by a system administrator from the GUI. These role-based workgroups be used to configure access and modification privileges to all ports and filters	10	Select	0	
49	The Solution must be able to provide Control access to individual network ports, tool ports, and filters based on assigning users into groups	10	Select	0	
50	The Solution must support Restful Web based API - for automation - Adaptive Response	10	Select	0	
51	The Solution must support IP address whitelist to securely access management port.	10	Select	0	
52	The Solution must support to redirect to port 443 when receiving port 80 http access	10	Select	0	
53	The Solution support to use following RSA and ECDSA ciphers to enhance the security when connecting to Solution https UI. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,ECDSA TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,RSA	10	Select	0	
54	The Solution must support to disable http port 80 to access the management UI	10	Select	0	
55	The Solution must support IPv4 and IPv6 addresses to be configured on management port	10	Select	0	
56	The Solution must support to configure session timeout and login banner	10	Select	0	
57	The Solution must support the Government Security Compliances not limited to FIPS 140-2 (Level 1) or The Solution must support the use of standards-aligned cryptographic module	10	Select	0	
58	The Solution must support AAA using:				
58.1	TACACS+	10	Select	0	
58.2	RADIUS	10	Select	0	
58.3	LDAP	10	Select	0	

59	The Solution must support event notification using:	-	Select	0	
59.1	Syslog with configurable level, facility, L4 port	10	Select	0	
59.2	Syslog with TLS enable	10	Select	0	
59.3	Syslog to report to at least 5 servers	10	Select	0	
59.4	Syslog to report to IPv6 and IPv4 addresses	10	Select	0	
59.5	Support built-in Syslog viewer	10	Select	0	
59.6	SNMP traps v1, v2 and v3	10	Select	0	
59.7	Standard MIBs and IANA private Enterprise MIBs	10	Select	0	
59.8	Option to enable IPv6 SNMP	10	Select	0	
60	The Solution must support Multiple threshold crossing syslog event and traps can be setup on a port by port basis, e.g. the threshold can be based on port's Rx Utilization, Tx Utilization, Invalid packets, dropped packets...etc.	10	Select	0	
61	The Solution must provide statistics view from its GUI. Moreover statistics must be available be viewed by individual ports and filters as well as in summarized views of all ports and filters	10	Select	0	
62	The Solution must provide Inspected and passed statistics via the GUI at network ports, filters, and tool ports - including current, average, and peak statistics	10	Select	0	
63	The Solution must provide Invalid packet statistics at the network ports	10	Select	0	
64	The Solution must provide Real time graphing of statistics in the GUI	10	Select	0	
65	The Solution must support user Setting to choose the units for displaying statistics in the Web Console GUI. The units are not limited to bits per second (bps), kilobits per second (Kbps) and megabits per second (Mbps).	10	Select	0	
66	The Solution must be able to support export or import specific elements of configuration. (e.g. port or traffic configuration only)	10	Select	0	
67	The Solution must be able to support scheduled auto backup of configuration for standalone packet brokers.	10	Select	0	
68	The Solution must be able to support LLDP on each port to generate or receive LLDP packets from other devices. LLDP receive and/or transmit can be enabled or disabled on each individual port.	10	Select	0	
69	The Solution must provide a dashboard view without additional license or hardware in order to keep track of overall network performance or statistics, the info not limit to packet/session distribution among countries, applications, sites, threat intelligence...etc.	10	Select	0	
70	The Solution must be able to view the port transceivers and light power information via GUI or Web API on per port basis	10	Select	0	
71	The Solution must have an offline PC Simulation Tool that can be used to prepare configuration offline and then import to the production Solution	10	Select	0	
72	The Solution must support to schedule auto backup on ftp server	10	Select	0	
73	The Solution Vendor must provide a central management systems.	10	Select	0	
74	The Solution must support an option to provide multiple boxes Single Pane of Glass view and configure all ingress, egress ports and all filter options	10	Select	0	
F	Traffic Steering				
75	The Solution must support the following aggregation and replication profiles:				
75.1	One-to-One	10	Select	0	
75.2	One-to-Many	10	Select	0	
75.3	Many-to-One	10	Select	0	
75.4	Many-to-Many	10	Select	0	
76	The Solution must be able to support dynamic packet load balancing with "5-tuple based mechanism" and "weight base". And able to configure up to 48 x 1G/10G port per load balancing group	10	Select	0	
77	The Solution must be able to support dynamic packet load balancing with Tunneled MPLS inner IP address	10	Select	0	
78	The Solution must be able to configure all filtering capacities via GUI.	10	Select	0	
79	The Solution must be able to provide 3-stage Filtering capability at Ingress port, mid-level Filter and Egress port in an easy to use GUI	10	Select	0	
80	The Solution must calculate and handle Filter Rules Overlapping scenario automatically. When changes in filter rules were made, the Solution must recompiles all the filter rules without having user intervention on other non-related filter rules.	10	Select	0	
81	The Solution must be able to support IPv4, IPv6 filtering simultaneously	10	Select	0	
82	The Solution must support standard IP header field based filter rule	10	Select	0	
83	The Solution must support to filter with complex IP fragment criterion with an easy ready template, not limit to the options include: Non Fragment, First Fragment, Fragment not First.	10	Select	0	
84	The Solution must support custom filter rule and up to 128 bytes deep into Ethernet frame.	10	Select	0	

85	The Solution must support built-in custom filter rule templates for common non standard IP packets like MPLS, GTP and VxLAN.	10	Select	0	
86	The amount of Solution's filter memory on L2/L3, IPv4/IPv6, ingress port, mid-level filter and egress port must be able to configure and allocate manually	10	Select	0	
87	The Solution must be able to support at least up to 16000 filter rules, and additional 8000 source IPv4 rules and 8000 destination IPv4 rules.	10	Select	0	
88	The Solution must support extremely easy filter rule setup. e.g. range of IP address & port number rules can be entered as one statement like this "192.168.1.100-123:24-79", and range of VLAN id rule like this "34-61".	10	Select	0	
89	The Solution must support mapping and filtering traffic to a new egress port from any ingress port(s) currently mapped to egress port(s) with overlapping filters	10	Select	0	
90	The Solution must supports filtering on either outer VLAN (802.1Q) or inner VLAN tags (802.1 Q-in-Q double-tagged packets) at the Network port(Ingress), Dynamic filter(middle), and Tool port(Egress)	10	Select	0	
91	The Solution must provide users to copy / paste and modify filters to other filter collections. Moreover, filters created on one Solution must be able to copy/paste to other Solution	10	Select	0	
92	The Solution must be able to support line rate VxLAN and GRE Tunnel origination and termination.	10	Select	0	
93	The GRE tunnel termination must be able to support respond to PING or ARP	10	Select	0	
94	The Solution must be able to support to assign IP address on the network interface (or traffic ingress port)	10	Select	0	
95	The Solution must be able to support VLAN replacement, or tag an VLAN id on incoming traffic based on filter criteria condition(s).	10	Select	0	
G	Cluster features				
96	The cluster feature can be enabled by an optional license	10	Select	0	
97	The clustering must be able to support more than 1 controller node in a cluster domain	10	Select	0	
98	The clustering must be able to support LLDP auto discovery and creation of cluster interconnects.	10	Select	0	
99	The clustering must be able to support both single and multihop hop.	10	Select	0	
100	The clustering must be able to support automatic failover to alternative route	10	Select	0	
101	The clustering must be able to support different topologies not limited to Star, Hub-Spoke, leaf-spine, multiple aggregation layers, Ring and Dual Ring.	10	Select	0	
102	The clustering must be able to support multiple equal cost paths, and best routes are calculated based on least hop-count using Shortest Path First (SPF) algorithm.	10	Select	0	
103	The clustering must be able to support load balance traffic via multiple equal cost paths, but still guarantee session integrity and avoid packet reordering	10	Select	0	
104	The clustering must be able to support manual re-route optimization, and on-demand route optimization by the systems.	10	Select	0	
105	All clustering features available on UI can also be configured or modified via Restful API.	10	Select	0	
106	The clustering must support dual home tool, which it behaves like an active-standby architecture to protect against one of the link(or port group)/path failure. The switch over must be done automatically within the Solution(s), i.e. not relies on any scripting or external mechanism.	10	Select	0	
107	The two port instances on dual home tool support must be flexible enough to allow to be defined as per port or group of port basis.	10	Select	0	
108	The dual home tool must support traffic revertive, which auto switch back the traffic to the healed failed link (or port group / path)	10	Select	0	
109	The dual home tool must support to connect to just one Solution (with two ports configured to run as dual home mechanism or active-standby) or two Solution.	10	Select	0	
110	The clustering should allow to choose the interconnected link(s) with layer 2 or layer 3 (e.g. GRE) encapsulation type.	10	Select	0	
	SSL Orchestrator				
1	Physical Specification				
1.1	System must of be 19-inch rack mountable 1U/2U form factor	10	Select	0	
1.2	System must have dedicated management port	10	Select	0	
1.3	System must have 24 x 1/10 G and 1Option of 4 x 100 G ports	10	Select	0	
2	Performance				
2.1	System must support 150 K SSL offload CPS on RSA 2 K Key and 90 K SSL offload CPS on ECDHE cipher	10	Select	0	
2.2	System must support 50 K SSL CPS for SSLo	10	Select	0	
2.3	System must support 64 million concurrent IP sessions and 2 M SSL sessions	10	Select	0	
2.4	Syste must support L7 Connections per second - Atleast 3 Million	10	Select	0	
3	Partition/Virtual Context				
3.1	System must support 30 Partition/Virtual Context keeping in view that One virtual partition will do decryption and another will do re-encryption	10	Select	0	
3.2	System must support dedicated configuration file for each Virtual context	10	Select	0	

3.3	System must support resource allocation to each context including throughput, CPS, Concurrent connection,SSL throughput	10	Select	0	
3.4	System must be able to modify the resource allocation on the fly without restarting/rebooting any context	10	Select	0	
3.5	All the virtual context must be available from day-1	10	Select	0	
4	Security				
4.1	System must support protection from Fragmented packets	10	Select	0	
4.2	System must support protection from IP Option .The System should have in-built HSM or a third-party HSM supplied by the bidder, which must be integrated with the proposed solution	10	Select	0	
4.3	System must support protection from Land Attack	10	Select	0	
4.4	System must support protection from Packet Deformity Layer 3	10	Select	0	
4.5	System must support protection from Packet Deformity Layer 4	10	Select	0	
4.6	System must support protection from Ping of Death	10	Select	0	
4.7	System must support protection from TCP No Flag	10	Select	0	
4.8	System must support protection from TCP Syn Fin	10	Select	0	
4.9	System must support protection from TCP Syn Frag	10	Select	0	
4.10	System must support connection limit based on source IP	10	Select	0	
4.11	System must support connection rate limit based on source IP	10	Select	0	
4.12	System must support request rate limit based on source IP	10	Select	0	
4.13	SSL/TLS Interception", "REST API", and "programmable traffic policy scripting" (or equivalent)	10	Select	0	
4.14	Decrypted Traffic Isolation: Mandates that any traffic decrypted for inspection purposes is confined strictly to dedicated tool-facing interfaces used by monitoring/security tools, and is re-encrypted before it is allowed to leave that isolated segment. Decrypted (plaintext) traffic must never traverse or reach production network segments, eliminating any risk of customer data being accidentally exposed in the clear during the inspection process.	10	Select	0	
4.15	SSL/TLS Orchestrator Throughput (Gbps): The proposed solution should comply with the sustained throughput figure for the decrypt-inspect-re-encrypt cycle with all security features active simultaneously (rather than throughput under idealized or feature-disabled conditions)	10	Select	0	
4.16	STARTTLS & Non-HTTPS TLS Support: Extends TLS inspection coverage beyond generic "any TCP port" handling to explicitly guarantee support for opportunistic/STARTTLS-based TLS protocols — including SMTP (email transport), IMAP and POP3 (email retrieval), and FTPS (secure file transfer) ensuring visibility into encrypted enterprise messaging and file-transfer traffic that upgrades to TLS mid-session, which generic TCP inspection alone may not correctly handle.	10	Select	0	
4.17	Deploy an enterprise SSL Visibility and Orchestration platform capable of centralized SSL/TLS decryption, intelligent traffic classification, policy-based service chaining, health monitoring, high availability, and secure forwarding of decrypted traffic to one or more inline or out-of-band security inspection solutions.	10	Select	0	
5	Traffic redirection features				
5.1	System must support load-balancing of multiple security devices	10	Select	0	
5.2	System must support Explicit proxy functionality with proxy chaining	10	Select	0	
5.3	System must support traffic redetection based any L2-L7 parameters	10	Select	0	
6	SSL Insight features				
6.1	System must Outbound SSL interception	10	Select	0	
6.2	System must support L2 and L3 mode of deployment	10	Select	0	
6.3	System must support ICAP integration with DLP and AV	10	Select	0	
6.4	System must support modification of headers	10	Select	0	
6.5	System must support before proxy interception (between Client and Proxy)	10	Select	0	
6.6	System mst support SSL interception bypass based on source and/or destination IP	10	Select	0	
6.7	System mst support SSL interception bypass based SNI values	10	Select	0	
6.8	System mst support SSL interception bypass based URL category	10	Select	0	
6.9	System must support bump in a wire deployment mode	10	Select	0	
6.10	System must support interception of SSH traffic	10	Select	0	
6.11	System must support sending decrypted feed to up to 4 offpath devices	10	Select	0	
6.12	System must support dynamic SSL interception for SSL traffic on any tcp port	10	Select	0	
6.13	System must support URL blacklisting and whitelisting	10	Select	0	
6.14	System must support TCL based scripts for custom rules	10	Select	0	
7	Redundancy				
7.1	System must support VRRP based redundancy	10	Select	0	
7.2	System must support active-active and active-backup configuration	10	Select	0	
7.3	System must support automatic and manual configuration sync	10	Select	0	

7.4	System must support dynamic VRRP priority by traffic interface, server, next hop and routes	10	Select	0	
8	Management				
8.1	System must have Web-based Graphical User Interface (GUI)	10	Select	0	
8.2	System must have Industry-standard Command Line Interface (CLI)	10	Select	0	
8.3	System must support Granular Role-based/Object-based Access Control	10	Select	0	
8.4	System must support SNMP, Syslog, email alerts, NetFlow v9 and v10 (IPFIX), sFlow	10	Select	0	
8.5	System must support REST-style XML API (aXAPI) for all functions	10	Select	0	
8.6	System must support external authentication including LDAP, TACACS+, RADIUS	10	Select	0	
Total		1790		0	

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

Bidder & OEM to right size the solution, keeping in view the requirement and integration touchpoints mentioned in the RFP. The above requirement are minimal.

DNS Protection					
S. No.	Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A	General				
1	The DDI solution should offers a comprehensive and standards-based integrated solution for DNS, DHCP, and IPAM for both IPv4 and IPv6 protocols, ensuring robust and efficient network resource management in compliance with industry best practices.	10	Select	0	
2	The DDI solution should be a hardware appliance for DNS & DHCP and virtual appliance for IPAM and reporting, all from a single vendor.	10	Select	0	
3	The DDI solution must provide integrated, high-availability without any additional third-party software components and ensure automatic and seamless failover between all components.	10	Select	0	
4	The DDI solution should support SNMPv3 for discovery and monitoring purposes.	10	Select	0	
5	The DDI solution must be capable of synchronizing its time with multiple NTP servers	10	Select	0	
6	The DDI solution must be compatible with RADIUS, LDAP, and Active Directory.	10	Select	0	
7	The DDI solution should provide both GUI/ CLI based configuration.	10	Select	0	
8	The DDI solution offers seamless scalability through the addition of licenses	10	Select	0	
9	The DDI solution should offer flexible deployment options, including Master-Slave, Multi-Master, and Stealth Mode configurations.	10	Select	0	
10	The DDI solution should operate without the need for software agents or thick clients.	10	Select	0	
11	The DDI solution should support granular rights administration limiting the function and rights to user and Subnet level	10	Select	0	
12	The DDI solution should provide a web-based user interface that is independent of specific browser vendors, with a multi-tenant architecture. It must create different user profiles with different level of permissions. As an example, the roles must include:- (a) Administrator (b) Reporting user (c) Read-only users	10	Select	0	
13	The DDI Solution must provide real-time reports on system operation, maintain audit trails, and generate graphical representations of report data for DNS, DHCP, and IPAM.	10	Select	0	
14	The solution must have inbuilt detailed reports & analytics to monitor audit logs. Solution should also allow customization of the reports as per the user requirement.	10	Select	0	
15	DDI Reporting engine should include audit reports containing a timestamp, username and record modified.	10	Select	0	
16	The DDI solution should support the forwarding or redirection of solution logs to a specified syslog server(SIEM)	10	Select	0	
17	The DDI solution should be able to send the alerts, reports etc.	10	Select	0	
18	The solution must be supported Import Wizard for the DNS and DHCP Appliance and must not require any external Java program or external Virtual Machines	10	Select	0	
19	All the component including OS, licences, software components, databases etc. should be Enterprise-grade and be provided as part of solution.	10	Select	0	
20	The solution should have hardened OS with no root access.	10	Select	0	
21	The solution must support SIEM, NAC, VA, Firewall Integration. The integration must be ready template based or doable using API.	10	Select	0	
B	IP Address management				
22	The IPAM solution should act as Central management Server for proposed DNS & DHCP Server from single vendor & should have inbuilt reporting for IPAM Appliance	10	Select	0	
23	The IPAM appliance must be capable to control DNS and DHCP servers distributed anywhere.	10	Select	0	
24	IPAM must support following functionalities:- (a) Create group. (b) Create Subnet. (c) Add subnet to group. (d) Scanning L3 and L2 devices in the network.. (e) IP address scanning within the subnet. (f) IP address scanning within the group. (g) Display device name with IP address. (i) Automatically detect devices. (i) Manually adding the device.	10	Select	0	

25	IPAM solution must show following IP Details:- (a) IP Address. (b) DNS name. (c) Last alive time. (d) Status(used, unused). (e) Should show contact details of administration(Manual Entry). (f) Contact person name(Manual Entry) (g) Contact person phone number(Manual Entry). (h) Location name(Manual Entry). (i) Should show device details.	10	Select	0	
26	The IPAM solution should be able to seamlessly integrate with DNS and DHCP Records	10	Select	0	
27	The solution must be flexible to allow the creation of custom fields for objects in IPAM. This must be configurable via the Web GUI.	10	Select	0	
28	The solution must include an application programming interface (API) in order to interface with network and/or asset management solutions, a configuration management database (CMDB) solution or other applications.	10	Select	0	
29	IPAM solution must perform Auto discovery of network devices i.e., L3 and L2 devices using a variety of methods including SNMP, ICMP etc.	10	Select	0	
30	The IPAM solution should be able to create its own gadget to display customized subnet reports, free IP, used IP.	10	Select	0	
31	The IPAM solution should have the ability to locate the available subnets inside a Supernet. This is to provide assistance to users when creating subnets inside an aggregated Network.	10	Select	0	
32	IPAM solution should support VLSM (Variable Length Subnet Masks)	10	Select	0	
33	IPAM solution should be able to export reports in PDF, CSV, XLS, XLSX formats	10	Select	0	
34	IPAM solution should have support for workflow process for various administrator roles and should include a change approval oversight capability.	10	Select	0	
35	The Solution must have the capability to find free address space across a range, automate the transition between IPv4 and IPv6 and provide automation to eliminate IP conflicts and configuration errors.	10	Select	0	
36	The IPAM solution component must perform host discovery using a variety of methods not limited to ping, Address Resolution Protocol (ARP) via SNMP protocol for 3000 number of L3 and L2 devices	10	Select	0	
37	The IPAM must provide clientless/Agentless integration (using APIs or any other method) with VMware Vcenter/Vsphere, Microsoft Hyper-V, Nutanix AHV, Red Hat OpenStack & OpenShift or any other Virtualization Platform, Public Clouds (i.e., GCP, AWS, Azure etc.)	10	Select	0	
38	IPAM must automate the discovery of free IP address space, support dynamic network reconfiguration through subnet division and merging, and identify potential IP address conflicts. The tool should also provide quick and efficient search capabilities.	10	Select	0	
39	The IPAM must be able to perform and track address space allocations in accordance with routing topology to model and optimize route aggregation.	10	Select	0	
40	IPAM must be able to visualize the network topology in hierarchical or in tree form.	10	Select	0	
41	The IPAM should offer rapid search functionality, enabling users to quickly find specific information, including lease history.	10	Select	0	
42	IPAM must provide centralized inventory reporting showing which device is assigned to which IP address within the network.	10	Select	0	
43	There must be provision to configure role based and object based access control with different access profiles (per group, allowing access per customer, per network etc.)It must also be possible to define address space authority boundaries per group.	10	Select	0	
44	IPAM must have adequate security tools to avoid any unauthorized access to the system in particular and solution as a whole.	10	Select	0	

45	Hierarchical mapping of sites (i.e. Entity) in sequence of Head Office -> Regional/State Office -> Location must be supported in IPAM and must have following features but not limited to, and display as a single dashboard:- (A) Location Management - Creation of Location - Location ID - Location Name - Location Description - Controlling Office - IP Subnet - Entity Status (Static/Mobile) - Remarks - Update Location Information - List of location (B) IP Subnet Management - IP Block Allocation - Start IP Address - End IP Address - Subnet Mask - Remark - IP Subnet Allocation - Selection of IP Block/Service. - Release IP Address from Subnet Block and linking to: - Entity - Start IP Address and End IP Address with Subnet Mask - Selection of VRF and VLAN for linking release IP Address. - Release of IP Address - IP Subnet delete - IP Subnet update - Remarks	10	Select	0	
46	IPAM must be fully integratable with the DHCP system with the capability to fetch all the scopes that are defined in the DHCP Server and display the total, used, and available IP Addresses in each scope. When the number of available IP addresses falls below a defined value, the display should indicate the criticality.	10	Select	0	
C	DHCP server				
47	The DHCP server must have address assignment, both stateless and stateful configuration and prefix delegation for full IPv4 and IPv6 address management.	10	Select	0	
48	The solution must track and log all user changes to DHCP configurations. The audit logs must be able to identify the change(s) made, the user/solution making the change, and a timestamp.	10	Select	0	
49	The system must support all the three mechanism for allocation of IP address to the client. i.e. Automatic, Dynamic and Manual.	10	Select	0	
50	The solution must graph (visually display) the different scopes based on number of IP's used/available over a set period of time	10	Select	0	
51	The DHCP solution must support one IP per MAC address (one lease per client).	10	Select	0	
52	The DHCP solution must be able to release the DHCP lease if the MAC address has moved to another IP	10	Select	0	
53	The solution must provide device finger printing and display or report the data in the GUI	10	Select	0	
54	The solution must support creating DHCP custom options.	10	Select	0	
55	The DHCP solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses	10	Select	0	
56	The solution must provide the ability to detect or block devices attempting to use DHCP based on various attributes. These attributes must include MAC address but can include device fingerprint, DHCP options, etc	10	Select	0	
57	The DHCP solution must integrate to DNS and IPAM for lease consolidation and capacity planning	10	Select	0	
58	The DHCP solution must have its built-in security mechanism against Rogue Clients performing DHCP Storm attacks without the need for additional licenses	10	Select	0	
59	The DHCP solution must be able to send alerts in case of DHCP related attacks	10	Select	0	
60	The DHCP should not require server on each subnet. To allow for scale and economy, DHCP must work across routers or through the intervention of BOOTP relay agent and DHCP must interoperate with the BOOTP relay agent.	10	Select	0	
D	Architectural Requirements				
61	The proposed solution must be based mandatorily on recursive and authoritative DNS analysis	10	Select	0	
62	The solution must have DNS security and DNS license for 45K QPS from day one, user can be remote and/or on-premise.	10	Select	0	

63	The proposed solution should provide integrated DNS, DHCP and IP Address Management (IPAM) functionality, but not limited: DHCP: Dynamic IP assignment, IP lease management and reservation, failover, IPv4/IPv6 support IPAM: Centralized IP inventory, conflict detection, audit, subnet planning, Integration with DHCP and DNS for end-to-end IP lifecycle management DNS: Authoritative server, DNSSEC, ACLs, logging, rate limiting, Dynamic DNS (DDNS) integration with DHCP.	10	Select	0	
64	DNS Security solution should be placed separately in DMZ (in HA in Bank's premise) should provide bank the following: a) Security administration – Choice of algorithms and key sizes (TSIG and DNSSEC) – Key management (generation, storage, and usage) – Public key publishing and setting up trust anchors – Key rollovers (scheduled and emergency). b) The platform should support both primary and secondary nameservers. c) The solution should support DNS Response caching d) Proposed Solution should mitigate DNS Security attacks like Cache poisoning , DDoS, data exfiltration etc. e) The solution should support export of logs to Bank on SIEM tool	10	Select	0	
65	The threat intelligence must be consumed from on-premises for Authoritative, Recursive and Caching DNS	10	Select	0	
66	The solution should have IPV6 support with DNS 6 to DNS 4 & DNS 4 to DNS 6 translation based health check for intelligent traffic routing and failover. Solution should support full DNS server functionality to support all kind of DNS records including A, AAAA, MX, CNAME, PTR DNS records.	10	Select	0	
67	The solution should support Multi-homing function for inbound IPv4 and/or IPv6 traffic Load Balancing by enabling DNS relay or DNS authoritative server function.	10	Select	0	
68	The solution must be applicable simultaneously to corporate users connecting from wired and wireless networks, with the possibility to define different policies based on different public IPs, and or internal networks	10	Select	0	
69	The Solution should support MicrosoftAD DNS integration.	10	Select	0	
D	Security Requirements				
70	The solution must be able to detect and block advanced malware related domains regardless of the specific ports or protocols used by the malware	10	Select	0	
71	The solution must be able to detect and block malicious domains using protocols different from HTTP/HTTPS	10	Select	0	
72	The solution must be able to block at least from the following categories of malicious domains: botnets, exploit kits, drive-by, phishing, newly seen domains	10	Select	0	
73	The solution must be able to prevent infections, blocking the DNS requests towards malware distribution domains or drive-by domains, and contain the pre-existing infections, blocking the DNS requests towards command and control infrastructures. The solution should support following Feeds :				
73.1	Base Hostnames	10	Select	0	
73.2	Anti-malware	10	Select	0	
73.3	Ransomware	10	Select	0	
73.4	Bogon	10	Select	0	
73.5	Malware Ips/Domains	10	Select	0	
73.6	Bot IPs/Domains	10	Select	0	
73.7	Exploit Kit IPs/Domains	10	Select	0	
73.8	Malware DGA hostnames	10	Select	0	
73.9	TOR Exit Node IPs/Domains	10	Select	0	
74.10	Extended Base & anti-malware Hostnames	10	Select	0	
74.11	Extended malware IPs /Domains	10	Select	0	
74.12	Extended TOR Exit Node IPs /Domains	10	Select	0	
74.13	Extended Ransomware IPs /Domains	10	Select	0	
74.14	Extended Exploit Kits IPs/Domains	10	Select	0	
74.15	SpamBot IPs/Domains	10	Select	0	
74.16	Spambot IPs DNSB/Domains	10	Select	0	
74	The Solution should have the ability to Log, Block & Quarantine poorly behaving clients based on their DNS Transactions.	10	Select	0	
75	The solution must leverage predictive intelligence and not just use static signatures or blacklists	10	Select	0	
76	The threat intelligence must be automatically updated after the discovery of a new threat without any manual update operations. The Threat Intelligence should be updated as soon as provided by the OEM	10	Select	0	
77	The vendor shall have an in-house threat research team to provide real-time intelligence and not depend on third party feeds or lists	10	Select	0	
78	The proposed solution must support Threat Intelligence based on Behavioral Analysis and Machine learning.	10	Select	0	
79	The Solution should have security policy to prevent from DNS Based Fast attacks using Hold down feature, Recursive Query Timeout, Fetches per server, Fetches per zone without any additional license.	10	Select	0	
E	Management Requirements				

80	The management interface must be web-based with a multi-tenant architecture. It must allow to create different user profiles with different level of permissions. As an example, the roles must include:				
80.1	Administrator	10	Select	0	
80.2	Reporting User	10	Select	0	
80.3	Read-Only Users	10	Select	0	
81	The policy editor must allow the creation of security policies.	10	Select	0	
82	The policy editor must allow to define a blocking page for the blocked DNS connections	10	Select	0	
83	The policy editor must allow to forward the blocked connection to an internal URLs	10	Select	0	
84	The events related to all the DNS queries analyzed must appear in real time, with the ability to configure filters based on destination, source IP, response type and date	10	Select	0	
85	The Solution must support the prevention from Data Exfiltration over DNS with Behavioral Analysis / DNS Tunneling VPN	10	Select	0	
86	The Solution must support the Security policy to prevent from Domain Generation Algorithm based Attacks	10	Select	0	
87	The Solution should have security policy to prevent from DNS Based Fast Flux attacks	10	Select	0	
88	Proposed solution should provide SOC team capability to access threat intelligence for view of relationship between domains, IP and malware for investigation	10	Select	0	
89	All the activities made by administrators must be logged inside an Admin Audit Log Report	10	Select	0	
90	The Solution should support high speed query logging without any performance impact.	10	Select	0	
91	The management platform must allow to generate the following reports:				
91.1	Total requests	10	Select	0	
91.2	Activity volume	10	Select	0	
91.3	Top Domains	10	Select	0	
92	The Vendor must have Technical Assistance Center in India	10	Select	0	
93	The vendor must have support center in India	10	Select	0	
F	3rd Party Security Integration				
94	SIEM - DNS security event correlation	10	Select	0	
95	NAC - automating and deployment of NAC policies to malware infected client, identified by DNS security	10	Select	0	
96	The solution should provide the integration with Next Generation firewall, automated integration with End Point Security Solution, VA integration, SOAR Integration, NAC Integration, SIEM Integration, Web gateway solution.	10	Select	0	
97	The solution should provide the integration with Next Generation firewall, automated integration with End Point Security Solution, VA integration, SOAR Integration, NAC Integration, SIEM Integration	10	Select	0	
98	The Solution should have integrated GSLB functionality to provide DC-DR Failover.	10	Select	0	
99	The Central Management should Manage IPAM, DNS and DNS Security Solution	10	Select	0	
100	The Vendor should have TAC Center in India & should provide 24X7X365 TAC support	10	Select	0	
G	Deployment				
101.1	DHCP service should support dynamic IP assignment, IP lease management, reservation, and failover as per the RFP.	10	Select	0	
101.2	The proposed solution, however, should be capable of providing integrated DNS, DHCP, and IPAM functionalities as a unified platform, to ensure centralized management and future scalability.	10	Select	0	
101.3	The proposed solution should enable centralized management and reporting of DNS, DHCP, and IPAM, even if the services are hosted on separate nodes or zones	10	Select	0	
101.4	The solution should also support IPv4 and IPv6 DHCP scopes	10	Select	0	
101.5	IPAM solution to manage and monitor the entire internal IPv4 and IPv6 address space used across its branches, data centers, and offices.	10	Select	0	
101.6	The proposed solution should forward the internal DNS resolution request to AD and for external it should forward the same to recursive DNS instance proposed by the bidder. The solution should handle all the DNS request (internal and external) to be forwarded from all the assets.	10	Select	0	
Total		1250		0	

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

Web Gateway					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A	Centralized Proxy Solution				
1	The solution should be on premise appliance based and must Provide Web Proxy, Caching, Web based Reputation filtering, URL filtering, Antivirus, Antimalware, Enterprise Data protection control with minimum 1500 templates inbuilt with English Language support, Application Visibility & control, Detail Reporting and Management. Load balancing should be inbuilt in the appliance or should work with Bank's existing load balancer with no additional cost.	10	Select	0	
2	Provide safe internet access to users from advance threats and Protect from Legal liability, Security Risk and reduce Network Bandwidth Loss and Productivity Loss.	10	Select	0	
3	The solution should be capable of working in the following configurations: Standalone Explicit Proxy/Forward Proxy and Transparent proxy with option to enforce policies to detect low and slow data leaks (through integration with DLP) from day1 by overall solution. The Solution should provide categorization of all categories into different risk classes like productivity loss, Network Bandwidth loss, Legal legibility, security risk, business usage.	10	Select	0	
4	The solution should provide the SSL decryption ability within the appliance itself and should be able to inspect malicious information leaks even over SSL by decrypting SSL natively and Data exfiltration control asked in the RFP should natively be applied on same hardware. The appliance should have provision of separate Network Interface for Management ports and Data ports.	10	Select	0	
5	Solution should be capable of seamless integration with existing security devices and tools present such as AD (Active Directory), SIEM etc. And must able to seamlessly integrate with Web DLP solution proposed in the tender.	10	Select	0	
6	Solution should be integrated with SIEM applications and other security solutions of Bank.	10	Select	0	
7	The solution should support configuring scheduled automatic/scheduled backup of system configuration.	10	Select	0	
8	The solution should integrate with LDAP directory like Active Directory, for user authentication and authorization and enable application based policy definition per user or group.	10	Select	0	
9	The solution should be capable of terminating open session based on session and inactivity timeout values and should be able to set a definite time duration of a policy based on a user or group policy.	10	Select	0	
10	Solution should be able bypass the cloud based email service used in the bank. The proposed solution should support all standard protocols including FTP, HTTP, SOCKS and HTTPS proxy. Solution should be able to integrate, support, and handle architecture with PAC file solution to divert traffic of intranet (do not proxy) and internet.	10	Select	0	
11	Single solution or combination of solution proposed should have proxy & caching with URL filtering. Also provides Real time content classification, categorization and security scanning in built with proxy solution. Proxy filtering and Web Data security for on prem bank user's must run on same appliance.	10	Select	0	
12	Data flow visibility and protection through proxy should be integrate or inbuilt functionality of Web Security functionality i.e. controlling and Protecting of sensitive data movement.	10	Select	0	
13	Bidder to ensure that the proposed solution must integrate with DLP solution to provide protection over web channel in form of Exact data matching and index data machine along with structure data and unstructured should match with the help of fingerprints, keywords, dictionaries, machine learning, and destination URL category wise.	10	Select	0	
14	Solution should have strong Content filtering database. Solution should provide real time threats updates, new signatures and URL database like blacklisted Phishing, Malicious sites, Porn sites, terrorist sites, Religion based sites, Gambling sites, Hacking sites, anonym zing websites, anonymizing tools sites, anonymizing proxies sites, advanced malware command and control sites, advanced malware payloads sites, C&C communication sites, Bot networks sites, Compromised websites, key loggers, Ransomware detection and other identified fraud/malicious websites. Solution should have capabilities to detect and prevent accessing domains like phishing and malicious domains and must have the URL categories like Generative AI – Multimedia, Conversation and Text & Code and other AI ML Applications to control/block.	10	Select	0	
15	Solution should have web protection mechanism to identify and block web pages having malicious java script, VB script, executable, malicious or unauthorized ActiveX applications, potentially harmful programs or software's download and shareware.	10	Select	0	
16	The solution should support the templates for detecting the Dark/Deep Web URLs like .onion/.tor, encrypted attachments to competitors, Password Dissemination, User Traffic over time, Unknown Encrypted File Formats Detection. The solution should support detection of PKCS #12 files (.p12, .pfx) that are commonly used to bundle a private key with its X.509 certificate.	10	Select	0	
17	Should have a separate centralized and powerful management which should enable to deploy, view and control secure web gateway through a single console	10	Select	0	
18	The solution should apply security policy to more than 100 protocols in multiple categories more than 15. This includes the ability to allow, block, log, and assign quota time for IM, P2P, and streaming media and solution should provide at least below mentioned security categories from Day1:				
18.1	1) Advanced Malware Command and Control category	10	Select	0	
18.2	2) Advanced Malware payload detection category	10	Select	0	
18.3	3) Malicious embedded links and iframe detection category	10	Select	0	
18.4	4) Mobile malware category	10	Select	0	
18.5	5) Key logger and Spyware category	10	Select	0	
18.6	6) P2P software database	10	Select	0	
18.7	7) AI ML Applications to control/block	10	Select	0	
18.8	8)Generative AI – Multimedia, Conversation and Text & Code	10	Select	0	
19	Ability to create granular security policy definitions per user and groups to identify, block or limit usage of web categories or applications and widgets like instant messaging, social networking, video streaming, games and more. The solution should support granular classification of websites at a category level based on content and threat.	10	Select	0	
20	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links etc. simultaneously on a single solution.	10	Select	0	
21	Solution should have Proxy cache features and Content-filtering. Solution should support 2FA for administration for secure login or integration with other authentication solution	10	Select	0	
22	Solution should have integrate with proposed critical data protection solution in the RFP natively over web channel from day 1. Should be able to put control based on the URL categories and Geo locations both for normal text and textual images. Solution should also provide the indicators of compromise templates to protect critical data protection.	10	Select	0	
23	Solution should be able to restrict Users to download certain file types based on extension. Further it should also support capability of blocking true type executables.	10	Select	0	

24	Solution should provide application function control to identify, allow, block or limit usage of applications and features within them and protect environments with social media & internet applications.	10	Select	0	
25	Solution should identify and control the application based on the application database and application risk.	10	Select	0	
26	The solution must support different types of compression algorithms and scan nested compressed files.	10	Select	0	
27	The solution should support real time graphical and chart based dashboard for the summary of activities over Web.	10	Select	0	
28	Solution should have capabilities to configure User, IPs, URLs and Domains to Black list or white list/ exceptions for detections	10	Select	0	
29	Solution should be able to provide safe search, application blocking, URL re-categorization option and should report incident with URL category information along with user, IP, content violating policy etc.	10	Select	0	
30	Multiple accesses provisioning for same user using single policy instead of creating multiple policies or multiple access control lists for same user and IP.	10	Select	0	
31	Solution should be able to restrict User to access internet, during specified hours / time. (Time based revocation).	10	Select	0	
32	Solution must support detection and protection predefined ML for both images and documents like PII, Aadhaar etc., with add on if required from Day 1	10	Select	0	
33	The solution should have facility for End User to report Misc. categorization in URL Category via custom block page or equivalent technology	10	Select	0	
34	Solution should support natively integrate with Data protection tool offered in the RFP and must be able provide predefined template including region & Industry specific, India IT Act , Aadhaar No, PCI-DSS, Data Theft Indicator templates, templates to identify Disgruntled employees, templates to identify suspected emails to self, Templates for Cyberbullying and self destructive patterns, passwords files and suspicious behavior that is indicative of malicious activity, suspicious User Activity like detects data sent at an unusual time and must support multiple languages not only limited to English and Hindi etc.	10	Select	0	
35	The solution should provide proxy, caching, content filtering, SSL inspection, inline AV(Anti-Virus) protocol filtering. The solution should have more than 1500+ predefined templates to prevent the confidential information in block mode with the visibility to provide the sanctioned and unsanctioned application visibility and control. Solution should provide the details and reports for the data exfiltration happening in the password and encrypted files uploads over the web natively.	10	Select	0	
36	The Solution should be designed for user base request to web gateway deployed in active-active mode, managed through centralized management console. Bidder to factor multiple appliance to cater the load in the DC and DR location..	10	Select	0	
37	The proposed solution's operating system should be secure and free from vulnerabilities. The operating system security should not be subjected to third party vendor patch releases but should be Proxy Vendor's own proprietary or hardened Operating System.	10	Select	0	
38	In case more than one device is provided to cater to the above requirements, then it should have the capability to sync all configuration between all devices in case changes are being made on one device from a single management console. The syncing in case requires any external device then the same is to be provided free of cost	10	Select	0	
39	The proposed solution's proxy gateway should be a hardware appliance for Secure Web Gateway solution and should not be dependent on virtualization platforms. However any other component required to run the solution like management, DB, etc. can be provided as software but bidder to provision the required compute.	10	Select	0	
40	The proposed solution should not allows client IPs to be part of multiple policies, URL's in multiple categories whereas it should allow Client and URL to be part of one policy and category only for better security posture. The Solution should have a pre-defined privacy category group to enforce SSL decryption bypass based on the regulatory requirements.	10	Select	0	
41	The solution should detect and evaluate connections from servers with questionable or untrusted certificates.	10	Select	0	
42	The solution should have an application program interface (API) or using OEM Integration Methodology is provided to create categories and populate them with URLs and IP addresses for use in policy enforcement apart from minimum 95+ predefined categories. The solution also support all decrypted HTTPS traffic to a physical network interface to allows a trusted service device to inspect and analyze the decrypted data for its own purpose, without adding extra decryption products All Component should be factored by the bidder to meet the above requirement from Day 1.	10	Select	0	
39	The proposed solution should store and Process all Proxy policies and configurations locally on the proposed hardware appliances or in the solution and should not leave bank's premises at any point of time.	10	Select	0	
40	Bidder to ensure the migration from Bank's existing proxy to the new solution should be seamless	10	Select	0	
41	The solution should have granular control over popular social web applications like Facebook, LinkedIn, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to social media sites	10	Select	0	
42	The proposed Secure Web Gateway (SWG) solution shall support implementation of web security controls in alignment with applicable CERT-In Directions, Guidelines, and Advisories by providing URL filtering, web reputation analysis, malicious domain and IP blocking, DNS security, phishing protection, malware inspection, file-type control, SSL/TLS inspection (where permitted), and automated threat intelligence updates to protect users from internet and web-based cyber threats.	10	Select	0	
43	The proposed Secure Web Gateway (SWG) solution shall automatically consume and enforce updated threat intelligence to block access to newly identified malicious websites, phishing domains, command-and-control (C2) servers, malicious downloads, exploit-hosting websites, and other web-based threats without requiring manual policy intervention, thereby enabling rapid protection against emerging cyber threats in accordance with CERT-In advisories.	10	Select	0	
44	The proposed Secure Web Gateway (SWG) solution shall detect and prevent web-based zero-day and previously unknown threats using a combination of real-time threat intelligence, reputation services, behavioural analysis, and content inspection to reduce exposure to emerging internet-borne attacks.	10	Select	0	

45	The proposed Secure Web Gateway (SWG) solution shall enforce granular web access policies based on users, groups, devices, applications, URL categories, destination reputation, risk level, and content type, with the capability to log, monitor, and report all web access events for security monitoring and regulatory compliance.	10	Select	0	
46	The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution				
B SSL Capabilities					
47	SSL decryption inbuilt with proxy solution to scan HTTPS & tunnel protocol traffic. Should be able to intercept, decrypt and re-encrypt SSL/TLS, Decrypt outbound SSL. Solution must provide decryption of unverified encrypted traffic for scanning and then re-encrypt it before sending.	10	Select	0	
48	Solution shall support the following remote access capabilities on its management interface via HTTPS or SSH access and shall support role-based administration such as Administrator, operator , Read-only access user etc.	10	Select	0	
49	The solution should have capability to enable 100% SSL decryption without any compromise on the Proxy performance and Internet access speed performance.	10	Select	0	
C Access Log and Reporting					
50	Solution shall provide forensic evidence investigative reporting on the infection's activity within the network while accessing internet as follow: Event timestamp, network/Web events in sequence, suspicious communication, malware type, severity, source and destination of attack.	10	Select	0	
51	Should have ability to manage security environment through intuitive graphical interface which should provide views, details and reports on security health through a comprehensive, centralized security dashboard.	10	Select	0	
52	Solution should provide advanced threat dashboard to track the infection or threat history for User/IP, with the ability to access all forensic evidence for past infections over dashboard and detailed logs view	10	Select	0	
53	Solution should have built in various reports and can create custom reports like Executive report, Top users report, Top 10 reports for various category and Health reports etc.	10	Select	0	
54	Solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time).	10	Select	0	
D User Management and Policy Administration					
55	Solution should have dedicated centralized management architecture with web UI /GUI based dashboard console to monitor, reporting, notification, maintaining and policy push for the users centrally for multiple boxes/ solution/solutions	10	Select	0	
56	Organization should have the power to create detailed policies that should be based on the characteristics such as user identity, user role and specific aspects of a web application.	10	Select	0	
57	The user interface and system configuration of the management console should be comprehensive, flexible and easy to use such that it should be possible to provide the complete threat details.	10	Select	0	
58	There should be advanced user and application controls such as ability to expand user groups, domain names as well as detailed user and application usage information in reports, logs and statistics.	10	Select	0	
59	The solution must support granular access control and authorization to facilitate gathering of logs of user's access General Features and Policies.	10	Select	0	
E Licensing					
60	The licensing of the Solution should be User based, as per Bank's requirement.	10	Select	0	
61	The Solution should have perpetual/subscription/term based license with deployment on premise without any extra license cost to the bank for the entire duration of the contract	10	Select	0	
Total		710		0	

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

Zero Day Attack Protection for endpoint and network					
S.No	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Solution must be able to handle minimum of 10 Gbps of traffic capacity.	10	Select	0	
2	The proposed solution should support capabilities to monitor traffic from multiple segments like WAN, DMZ, Server Farm, Wi-Fi network, MPLS links, traffic from third party/perimeter firewall mentioned in the RFP etc. simultaneously on a single appliance.	10	Select	0	
3	The proposed solution should have capabilities to configure files, IP, URLs and Domains to Black list or white list.	10	Select	0	
4	The Proposed solution should provide correlated threat data such as: IP addresses, DNS domain names, URLs, Filenames, Process names, Windows Registry entries, File hashes, Malware detections and Malware families through a dashboard	10	Select	0	
5	The proposed solution must be able to provide intelligence feed for malware information, threat profile and containment remediation recommendations where applicable.	10	Select	0	
6	The proposed solution should be able to support XFF (X-Forwarded-For) to identify the IP Address of a host in a proxy/NAT environment.	10	Select	0	
7	Should detect lateral movement (attack activities) inside the network (beyond C&C connections)	10	Select	0	
8	Should have Advanced Threat Scan Engine to detect zero-day threats, embedded exploit code, rules for known vulnerabilities and enhanced parsers for handling file deformities	10	Select	0	
9	The proposed solution should have a built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency.	10	Select	0	
10	Solution should be deployed on premise along with on premise sandboxing capability and no data should be allowed to go on public cloud.	10	Select	0	
11	Solution must be a custom built on premise dedicated Anti-APT solution	10	Select	0	
12	Solution must generate analysis reports, suspicious object lists, PCAP files, and OpenIOC and STIX files that can be used in investigations	10	Select	0	
13	Should perform static and dynamic analysis to identify an object's notable characteristics: AutoStart or other system configuration, Anti-security and self-preservation, Deception and social engineering, File drop, download, sharing, or replication, Hijack, redirection, or data theft, Malformed, defective, or with known malware traits, Process, service, or memory object change and Rootkit, cloaking, Suspicious network or messaging activity	10	Select	0	
14	Should have extensive detection techniques utilize file, web, IP, mobile application reputation, heuristic analysis, advanced threat scanning, custom sandbox analysis, and correlated threat intelligence to detect ransomware, zero-day exploits, advanced malware, and attacker behavior.	10	Select	0	
15	Should detect from Targeted attacks and advanced threats, Targeted and known ransomware attacks, Zero-day malware and document exploits, Attacker behavior and network activity, Web threats, including exploits and drive-by downloads, Phishing, spear phishing, and other email threats, Data exfiltration, Bots, Trojans, worms, keyloggers and Disruptive applications	10	Select	0	
16	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Movement, Asset and data discovery and data Exfiltration.	10	Select	0	
17	Proposed solution should be able to provide customizable sandbox to match endpoint environments. Access different information about Affected Hosts on the following views: Displays a summary of affected hosts by attack phase, Provides access to Host Details views and Displays host event details in chronological order	10	Select	0	
18	Should display affected Hosts information that have been involved in one or more phases of a targeted attack	10	Select	0	
19	Should have combination of signature file-based scanning and heuristic rule-based scanning to detect and document exploits & threats used in targeted attacks including Detection of zero-day threats, Detection of embedded exploit code, Detection rules for known vulnerabilities and Enhanced parsers for handling file deformities	10	Select	0	
20	Should provide Threat execution and evaluation summary and In-depth tracking of malware actions and system impact, including the following: Network connections initiated, System file/registry modification and System injection behavior detection	10	Select	0	
21	Should have capability to do retrospective scan on CnC, Script Analyzer, Automatically send executable to sandbox.	10	Select	0	
22	The proposed solution should be able to detect lateral movement (East-West) of the attack without installing agents on endpoint/server machines with least 100+ protocols for inspection.	10	Select	0	
23	The Proposed solution should monitor Inter-VLAN traffic on a Port Mirror Session/TAP mode.	10	Select	0	
24	Should support extensive File Types i.e. Compressed Files (7z, rar, zip, cab, jar, gz, tar, bz2), Script Based (bat, ps1, vbs, js), Executables (exe, dll, scr) and Office Documents / PDF (doc / docx, ppt / pptx, xls /xlsx, pdf, mdb)	10	Select	0	
25	Should monitor all inbound and outbound network traffic	10	Select	0	
26	Proposed Sandboxing should use static, heuristic and behavior analysis, web, and file reputation, to detect ransomware and advanced threats	10	Select	0	
27	Solution should detect multi-stage malicious downloads, outbound connections and command and control from malicious attachments and URLs	10	Select	0	
28	Open Web Services API allows any product or authorized Technologies to submit samples and obtain detailed analysis and report	10	Select	0	
29	The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	10	Select	0	
30	Sandboxing environment should be securely isolated from the rest of the network to avoid malware propagation	10	Select	0	
31	Solution should support file analysis range, examines a wide range of all executables files, Microsoft Office, PDF, web content, and compressed file types using multiple detection engines and sandboxing	10	Select	0	
32	Sandbox appliance should have redundant power supply, 2 TB or more storage capacity (or as per OEM recommendation meeting the requirement mentioned in the RFP) with dedicated management port	10	Select	0	
33	The Proposed solution should be able to detect and analyze URLs which are embedded in MS office and PDF attachments	10	Select	0	
34	The Proposed Solution should be able to detect known bad URL before sandboxing	10	Select	0	
35	The Proposed solution should have options to define global recipients/contacts setting for alert/report	10	Select	0	
36	The Proposed Sandboxing solution must support analysis of Windows & Linux Operating System files	10	Select	0	
37	The proposed solution should support on premise centralized management for viewing information about detections	10	Select	0	
38	Solution should provide role-based access control for administration, investigation as well as operation purposes	10	Select	0	
39	Solution should be able to integrate with Microsoft Active Directory (AD) for account management	10	Select	0	
40	Solution should be able to centrally manage and deploy product updates including patches, hotfixes, and firmware upgrade	10	Select	0	
41	Solution should be able to centrally manage and deploy sandbox image update to managed products.	10	Select	0	

42	Solution should have a tree view, or equivalent view of managed products/devices, with the view above solution should be able to provide product/device name, IP address, connection status, and application versions.	10	Select	0	
43	Solution must provide granular log search filters for users to define their own search criteria	10	Select	0	
44	The solution central management should include various methods of sharing threat intelligence data with other products or services including TAXII / Web services.	10	Select	0	
45	Solution should integrate with Endpoint, Email and Server Security Solution for better Security posture and sharing of IOC's automatically, both user defined as well as the ones analyzed by sandbox	10	Select	0	
Total		40		0	

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

ZTNA					
S.No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	If any component of the proposed solution is hosted on a cloud platform, indicate whether the Product OEM/Cloud Service Provider (CSP) has submitted CSP compliance functional specifications and supporting documentation demonstrating compliance with all applicable requirements of this RFP. If the dropdown is not selected, the product will be considered NON COMPLIANT.		Select		
1	For On-Prem Users, the ZTNA solution should be deployed as a pair of Virtual Machines in each DC. DC1 and DC2 should be used in High-Availability in case one of the location has a downtime ensuring continuous productivity. This is to enforce ZTNA based access for On Prem Users (LAN, Branch to DC Internal App Access), etc.	10	Select	0	
2	Solution should be able to integrate with on-premises AD without any inbound internet exposure needed on the Firewall.	10	Select	0	
3	The ZTNA solution should have device posture validation across multiple parameters like Device Encryption, Registry Check, Process Check, AD Domain Check, OPSWAT and Certificates etc. to provide specific URL or Internet Access based on granular policy controls. The device posture check should be recurring and check the compliance of the posture periodically to maintain the Device Trust.	10	Select	0	
4	Any component installed in DC's (On-premise) must not need any inbound ACL rule in customer DC/DR Firewall to provide access to Private Application.	10	Select	0	
5	The Solution should have the capability to authenticate users and enroll/log in to the service using their Email Address. This capability should not need any SAML/SSO Integration and admin should be able to send invite links to the user's email to enable this functionality.	10	Select	0	
6	Solution should be able to integrate with SAML 2.0 (OKTA and ADFS etc.).	10	Select	0	
7	Solution should have Zero trust security and Digital Experience Management (DEM) from Day 1 using the same Endpoint Agent and single management console for both capabilities.	10	Select	0	
8	Solution should enable seamless access to Internal applications across multi-DC's (no need to connect any VPN/Remote Access Agent every time application access is required). The solution should be Always-On whenever Internet is reachable	10	Select	0	
9	Connectivity between remote users' devices and private applications should be secured by an end-to-end TLS encrypted tunnel.	10	Select	0	
10	The solution should have Granular policies for blocking or allowing access to private applications that can be built on criteria including User, Group or Organizational Unit (OU), Device Classification and Operating System.	10	Select	0	
11	The solution should provide the capability to add any number of App Connectors in DC without any additional price or license.	10	Select	0	
12	The End-user should not be able to see the Application Local IP even if they are authorized to access the application (application access based on FQDN but real Application IP is masked)	10	Select	0	
13	The ZTNA components including ZTNA broker, App Connector/Gateway should be deployed on-premises in SDC	10	Select	0	
14	The solution should support providing access to Internal Web Applications to contractors/third-parties without the need of installing any Agent on the contractor system. It should facilitate Private App Access via a Browser without any additional license from Day 1.	10	Select	0	
15	Solution should have dashboards providing information about Applications, Users, and System's Internal Components.	10	Select	0	
16	The Endpoint agent should be tampering proof and users should not be able to disable or uninstall the Client even with System Admin Right. Any application policy change on the Admin UI should reflect near real-time on the users.	10	Select	0	
17	user license should have unlimited bandwidth usage for with no capping from the OEM.	10	Select	0	
18	Solution should enable seamless access to Internal applications across DC-1/DC-2 (no need to connect/reconnect any VPN/Remote Access Agent every time application access is required). The solution should be Always-On whenever Internet is reachable.	10	Select	0	

19	Solution should be able to provide client/clientless Browser based access to Internal Web Applications from Day 1. It should also support the capability to enforce DLP policies on the access to Internal Web Applications.	10	Select	0	
20	The End point Agent should support multi-user mode installation (for ex. Installing agent on VDI/Thin Clients).	10	Select	0	
21	The solution should have a single Policy Engine with ZTNA and DEM in a unified/separate console. At any point in time, ZTNA features, and functionality sought should not be compromised. However, ZTNA and DEM should have “single agent deployment” in case agent-based solution deployment is proposed	10	Select	0	
22	The solution should support if required all endpoint- and server-initiated apps, like-to-like VPN replacement adding traffic optimization capabilities for enhanced performance and security.	10	Select	0	
23	The solution must support for client-initiated access to enterprise applications built on TCP and UDP protocols, thus enabling access to web applications and non-web / thick clients (e.g., SSH, RDP, Microsoft Windows Active Directory).	10	Select	0	
24	Solution must support Connector Dashboard provides insight into application traffic,app connector health, and utilization, enabling decision on resource allocation, connection optimization, and troubleshooting.	10	Select	0	
25	The solution should support Advanced Analytics report to provides real-time visibility into detailed application traffic and user activities, as well as alerting on policy violations	10	Select	0	
26	Solution should support extensive coverage with in-built Data types like Aadhar card, PII, etc with different File Types etc. Solution should support extensive coverage with 100+ in-built Data types with minimum 200 File Types.	10	Select	0	
27	Connectivity between remote users' devices and private applications should be secured by an end-to-end TLS encrypted tunnel and optimally routed through with a low latency, high-capacity, scalable network infrastructure.	10	Select	0	
28	Solution should have Granular policies for blocking or allowing access to private applications that can be built on criteria including User, Group or Organizational Unit (OU); Device Classification; or Operating System.	10	Select	0	
Total		280		0	

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

DLP					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A	DLP CENTRAL MANAGEMENT CONSOLE				
1	Proposed Solution should comply with the Digital Personal Data Protection Bill (data protection controls) during the contract period	10	Select	0	
2	Proposed solution should have highly scalable architecture with centralized management that integrates with data loss prevention for all the egress channels like endpoints, email and web channel	10	Select	0	
3	Central Management Console should be able to monitor the status, health and performance parameters, DLP policy posture and services on the endpoints.	10	Select	0	
4	All endpoints including desktops (Windows and non-Windows) and VPN laptops of the Bank should be monitored / managed through a single On-premises hosted orchestrator / management Server and console only.	10	Select	0	
5	Proposed solution should have a comprehensive list of pre-defined policies and templates with patterns to identify information pertaining to the Banking and Financial Institutions	10	Select	0	
6	The solution should allow creation of custom patterns and validators based on the bank's needs without any additional cost to the Bank.	10	Select	0	
7	Proposed solution should have capabilities of network DLP for configuration and management of DLP appliances from a single interface and should automatically distribute unified policies and rules to specific or all appliances.	10	Select	0	
8	Proposed solution should provide Out of the Box Rule Sets for country specific regulations where Bank has its presence.	10	Select	0	
9	Proposed solution should create policies that support full Boolean expression (Regex) for keywords/patterns.	10	Select	0	
10	Proposed solution should provide directory-based policies to selectively monitor / upload based on user, business units, active directory groups, specific groups of computers and specific groups of users.	10	Select	0	
11	Proposed solution should provide ability to configure policies to detect fingerprints and files from share / repository / date created etc. and define DLP policies for files being sent out of the organization via e-mail/ upload to website etc.	10	Select	0	
12	Proposed solution should have Role Based Access capabilities to create the user and assign specific roles (e.g. Admin, Read/write, Read only) for Management and maintenance of DLP solution and day to day Operation by the onsite Helpdesk team.	10	Select	0	
13	Proposed solution should be capable to manage and create DLP policies based on the country specific Data prevention laws and country specific sensitive data keywords.	10	Select	0	
14	The Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and also automatically learn false positives.	10	Select	0	
B	CONTENT DETECTION & CLASSIFICATION				
15	Solution should have the ability to Classify data based on the Confidentiality Levels and should have a default classification, suggested classification and classification based on the Regulations options as well	10	Select	0	
16	The solution should be able to classify unstructured data, namely word/excel/PowerPoint etc. and MS Outlook emails. The solution should be able to label the documents in headers/footers with a pre-selection capability for either header or footer or both. The solutions should be able to insert metadata tags in the documents and emails which can be read by DLP Solutions.	10	Select	0	
17	The solution must be able to detect Data Classification Labels applied by Data Classification partners by reading metadata as well as custom header analysis and supports writing metadata for interoperability. Solution should be capable of detecting the tags/labels defined by the third party data classification tools and block the data as per defined policies.	10	Select	0	
18	The Proposed solution should make sure that metadata is persistent i.e. any removed metadata is re-applied when the file is saved, printed or emailed	10	Select	0	
19	The Proposed Solution should provide the rules and policies to enforce around saving the documents and emails	10	Select	0	
20	The solution should allow powerful rule construction, using keywords and/or regular expressions in standard Boolean logic	10	Select	0	
21	Proposed solution should detect on pre-built dictionaries.	10	Select	0	
22	Proposed solution should detect and validate a wide range of sensitive data types (e.g., SSNs, CCNs, UID) for India and other foreign locations where PSB has its offices	10	Select	0	
23	Proposed solution should detect classified Proprietary File types (types that are not predefined) and on file content not on file extensions.	10	Select	0	
24	The solution should be able to monitor data copied to network file shares and should enforce structured and unstructured fingerprint policies even when disconnected from corporate network. It should be able to do full binary fingerprint of files and also able to detect even if partial information gets leaks from fingerprinted files or folders. Both structured and unstructured fingerprints should be stored on the endpoint itself and should perform all analysis locally without needing the network connectivity to reduce WAN overheads.	10	Select	0	
25	Solution should includes an endpoint agent that enables end user to manually/easily classify files and emails when they create.	10	Select	0	
26	Supports enforcing users to classify upon a file save or email send event, with flexibility to choose either automated, suggested or user-driven classification.	10	Select	0	
27	Provides the capability to automatically add headers, footers or watermarks in Office documents as well as PDF documents when users classify them.	10	Select	0	

28	Proposed solution should have capabilities with Single place to define classification and same should be used in Endpoint or network DLP to avoid defining same classification multiple times	10	Select	0	
29	In case of Policy violation, the solution should be able to retain all content/attachments in the transaction, not just the content that violated policy	10	Select	0	
30	The incident should include a clear indication of how the transmission or file violated policy (not just which policy was violated), including clear identification of which content triggered the match and should allow opening of original attachment directly from the UI	10	Select	0	
31	Proposed solution should be capable of discovery of confidential data on Windows, Non-Windows endpoints (desktops/laptops) E.g., Local files/Email files etc.	10	Select	0	
32	The DLP solution should be applicable for all structured and non-structured data across the Bank.	10	Select	0	
33	Proposed Solution should support data-labelling as defined by the bank during the data discovery & data classification .	10	Select	0	
34	The solution should have some guidance mechanism while user selects a classification level, to inform the users what is the context of a said classification level as per organization's policy.	10	Select	0	
35	The solution should have levels of actions Force, Warn, Log & Ignore classification and must provide the details of the user who classified the file and if any user is allowed to change classification, this change should be logged.	10	Select	0	
36	The solution should make sure that classification is written into the metadata of the document and can be customized as per the banks needs	10	Select	0	
37	The solution should provides a button in Word/ Excel/ PowerPoint/ Outlook ribbon which displays the classification of the file/email or/and allows users to select a classification label from a pop up window when clicked.	10	Select	0	
38	Administrators should be able to customize headers, footers and watermarks in terms of font type, font color, font size, text alignment (left, right, center). Besides including the classification label, the header, footer or watermark text should be customizable to include date/ time, email, username or machine ID at minimum.	10	Select	0	
39	The solution should have ability to automatically classify an email according to the classification of the attachment and block unclassified attachments from being sent.	10	Select	0	
40	The solution should provides suggestions to end users on an appropriate classification label based on content analysis of the Office document or Outlook email. The content analysis should be based on AI/ML or/and keywords/ regular expression.	10	Select	0	
41	Administrators should be able to customize the threshold for suggestions that are based on AI/ML confidence levels, so that suggestions are made only when AI/ML is more than X% confident of a particular label.	10	Select	0	
C ENDPOINT DLP					
42	Proposed solution should monitor/block data copied to removable storage devices (USB flash drive, CD/DVD, external hard disk etc.) and also should encrypt information copied to removable media with Native and Portable Encryption and manage the Encryption and DLP policies from the same management console.	10	Select	0	
43	Proposed solution should notify the end user of a policy violation using a customizable pop-up message and should capture content that violates a policy and store it in an evidence repository.	10	Select	0	
44	Proposed Solution should support the monitoring and blocking the printing on the Network or Local Printer	10	Select	0	
45	Proposed solution should be able to enforce policies while the endpoint system is disconnected from the corporate network and the endpoint agent should log all violations and reports into the central database when a connection to the corporate network is established.	10	Select	0	
46	Proposed solution should be able to Identify content using Regular Expressions, Key Words, Document Fingerprints, and patterns etc.	10	Select	0	
47	Proposed solution should be able to Identify content based on location and allow creation of policies based on Users and Groups.	10	Select	0	
48	Proposed solution should provide an option of rule override which can be authorized to use an override code issued from the security administrator based on the end user's justification or Policy/rule approved by Bank	10	Select	0	
49	Proposed solution should provide compliance report which will help to identify the DLP versions being deployed. This report can be used to identify If any EOL or older versions running in the Bank. Solution should have the feasibility to upgrade the systems to newer version from the same management console or by 3rd party software deployment tools used by the Bank.	10	Select	0	
50	Proposed solution DLP agent should protect itself from unauthorized removal or service stoppage. Uninstallation of DLP agent would require technical controls like one time password/ maker checker etc.	10	Select	0	
51	Proposed solution should Monitor/block email in MS Client.	10	Select	0	
52	Proposed solution should have an option to Encrypt / Quarantine / Monitor / classify sensitive files found during endpoint discovery.	10	Select	0	
53	Proposed solution should support Print Screen blocking on endpoint when configurable list of specific application are running, no matter it is in the foreground or background. The actual PrtScn evidence also should be submitted to the DLP system as forensic evidence.	10	Select	0	
54	Proposed solution should Monitor/block cut, copy or paste actions.	10	Select	0	
55	Proposed solution should Monitor/block data copied to network file shares	10	Select	0	
56	Proposed solution should Monitor/block policy violations based on metadata.	10	Select	0	
57	Proposed solution should be able to identify and block malicious activity like data thefts through files encrypted using non-standard algorithms and should be able to detect and block encrypted and password protected files without reading the encrypted content and also recursively inspect the content of compressed archives.	10	Select	0	

58	Proposed solution should support exceptions creation for user, group of users, URL/Domain, Applications etc.	10	Select	0	
59	Proposed solution should have multiple pre-defined applications and multiple application groups and allow application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture Also, solution should have the capability to define the third-party application.	10	Select	0	
60	Proposed solution should Provide "Cloud Storage Applications" group which monitors sensitive content accessed by these cloud storage application (i.e., one drive, share point, google drive, Box & iCloud) on the endpoint and prevent sensitive data from uploading to the cloud.	10	Select	0	
61	Proposed solution should be able to recursively inspect the content of normal compressed archives.	10	Select	0	
62	Proposed solution should be able to monitor and protect data classifiers created via the Fingerprinting of the structured and unstructured data.	10	Select	0	
63	Proposed solution should provide capabilities to identify data based on keywords or dictionaries and the solution should be able to enforce policies based on file types, size of files and the name of the file.	10	Select	0	
64	Proposed solution should Support multiple conditions by combining different data classifier, including Policy Template, Pattern, RegEx, Keyword, Dictionary, Scripts, and fingerprinting.	10	Select	0	
65	Proposed solution should be able to detect, monitor & block the data from scanned documents as per the DLP policies.	10	Select	0	
66	Proposed solution should be able to enforce different policies for desktops, laptops and group of systems.	10	Select	0	
67	Proposed solution should have ability to centrally define or change Endpoint Agent uninstallation and management passwords.	10	Select	0	
68	Agent should monitor and report last communication date & time with Central Management Server. It should also provide reports based on specific rule revision id.	10	Select	0	
69	Communications between agent and server should be encrypted and authenticated and Agent-Server authentication should be based on standard protocols (HTTPS/certificates) or encryption based.	10	Select	0	
70	Solution shall support to mask confidential data appearing in incident matches.	10	Select	0	
71	Proposed solution should support Mac & Windows OS like Windows (10, 11), Windows Server (2019, 2022 or higher), MacOS - Sonoma 14.0 - 14.7, Sequoia 15.0 - 15.4 and VDI: Citrix, VMware Horizon, etc.	10	Select	0	
72	Proposed solution should be interoperable with leading Antivirus / XDR solutions and OS without the need to downgrade or uninstall existing security solutions / OS	10	Select	0	
73	The solution should be capable to fingerprint the data generated from specific applications, Web URLs, Data Repositories, Network Shares	10	Select	0	
74	DLP solution should provide version details which can be used with Bank's Network Access Control (NAC) solution for compliance.	10	Select	0	
75	The solution should also have Data Theft Indicator policies/templates to detect/monitor Data Sent During Unusual Hours, Email to Competitors, Suspected Malware Communication, Suspected Malicious Dissemination etc.	10	Select	0	
76	The DLP solution should allow the Bank to configure the discovery scheduler option: once, daily, weekly or continuously and must support inclusion and exclusion by file type, folders, age or size. Also, endpoint should perform discovery only when the endpoint is connected to external power or Machine is Idle.	10	Select	0	
77	The DLP Solution should be capable to generate alert in case of transfer / upload of large files/ large amount of data	10	Select	0	
D Network Data Leakage Prevention (nDLP)					
78	Proposed solution should be provided with dedicated hardware appliances/Software Solution with all required hardware components for Email & Web DLP.	10	Select	0	
79	Proposed solution should intercept user requests for web destinations to identify critical & sensitive data uploads/data exfiltration and should be able to inspect malicious information leaks even over SSL by decrypting SSL natively.	10	Select	0	
80	Proposed solution should Monitor/block web (HTTP, HTTPS and FTP) transmissions via any browser.	10	Select	0	
81	Proposed solution should have native integration capabilities with web security gateway to inspect and prevent data loss through HTTP, HTTPS and FTP protocols.	10	Select	0	
82	Proposed solutions should have the feasibility to place Prevent Appliances in cluster mode to achieve redundancy	10	Select	0	
83	Proposed solution should have the capabilities of capturing the details of URL and user trying for data leakage through web posts.	10	Select	0	
84	Proposed solution should provide the ability to detect Policy violation which retains the source IP address, destination, username, user domain, protocol, and URL's.	10	Select	0	
85	The solution should be able to Discover and Monitor all the data and prevent the sensitive data leaving from the Bank.	10	Select	0	
86	The solution should support scanning of database such as Oracle, Microsoft SQL Server, and IBM DB2 etc.	10	Select	0	
87	Solution should support data at rest scanning for Exchange, Outlook PST, Databases, SharePoint, File systems, SMB, NFS and CIFS for Windows and non-windows based file shares.	10	Select	0	
88	The proposed solution work as a MTA to receive mails from mail server and inspect content before delivering mails to next hop and should quarantine emails that are in violation of company policy.	10	Select	0	
89	The solution should support Email DLP for Microsoft exchange on prem or O365 for all users and should be able to decrypt emails, attachments, and web or network files encrypted via Microsoft encryption for enhanced visibility and control. All licenses required for the same should be included and management should be from the same centralized management platform	10	Select	0	
90	The solution should support quarantine as an action for email policy violations and should allow the sender's manager to review the mail and provide permissions for him to release the mail without logging into the UI	10	Select	0	

E	Incident Workflow and Optical Character Recognition				
91	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc. Also should allow a role only to view incidents but not manage or remediate them.	10	Select	0	
92	In case of data infringement, DLP solution should support alert mechanism by email/other method to the reviewing authority. Reviewing/reporting authority should be able to view the data/file shared by the user, in order to take an informed decision.	10	Select	0	
93	The Solution should provide prioritized warnings and alerts regarding data leakage, as well as dashboards and reports. These include centralized and automated tools to provide automated incident response approaches and step-by-step workflows to investigate incidents.	10	Select	0	
94	The solution should have options for managing and remediating incidents through email by providing incident management options within the in the notification email itself.	10	Select	0	
95	The solution should provide Incident Workflow capabilities where user/Business Manager can remediate the DLP policy violations actions from handsets/emails without logging into the Management Console	10	Select	0	
96	Proposed solution should be capable in optical character recognition. OCR module should Detect image/pdf files. Identify the sensitive information available in these files. Allow/Block the files as per Bank DLP policies.	10	Select	0	
97	Solution should be manageable from a single management console for all DLP components	10	Select	0	
F	Incident Management & Reporting				
98	Proposed solution should provide the ability to detect Policy violation which retains the source IP address destination URL protocol, for all components of DLP solution.	10	Select	0	
99	The solution should also allow assigning of incidents to a specific incident manager	10	Select	0	
100	The incident should display the complete identity of the sender (Full name, Business unit, manager name etc.) and destination of transmission for all network and endpoint channels.	10	Select	0	
101	The solution should allow a specific incident manager to manage incidents of specific policy violation, specific user groups etc.	10	Select	0	
102	The solution should control incident access based on role and policy violated, also allow a role creation for not having rights to view the identity of the user and the forensics of the incident.	10	Select	0	
103	Proposed solution should provide the ability for Case content to be exported with full content and attachments for review by an external reviewer.	10	Select	0	
104	Proposed solution should have the provision to purge the incidents from the central management console based on defined criteria by the Bank. For example, purge incidents beyond 12 months or purge incidents related to particular policy.	10	Select	0	
105	Proposed Solutions should also have the provision to purge associated evidence files with the incidents from the central management console.	10	Select	0	
106	Proposed solution should generate reports in PDF, Excel, or CSV format.	10	Select	0	
107	Proposed solution should develop reports built around Banks requirements such as top Policy Violations, Senders, Content Type, Protocol, Historical Reports etc.	10	Select	0	
108	Proposed solution should be capable to store the infringement incident details for minimum 180 days or any duration stipulated by the regulator in an encrypted format.	10	Select	0	
109	Proposed solution should support integration with MS active directory for user authentication while DLP console login and fetching the user's details.	10	Select	0	
110	Proposed Solution should be capable of storing evidence generated against the DLP policy violations centrally as well as locally in encrypted form.	10	Select	0	
111	DLP Solution should be capable of integrating with Office365 for collecting DLP incidents (related to email DLP), incorporate these incidents with endpoint DLP and send consolidate data to Incident management portal.	10	Select	0	
112	DLP logs should not have any confidential/sensitive data in clear text. It should either be encrypted or masked	10	Select	0	
Total		1120		0	

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

DRM					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C6M/NC)	Calculated Score	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	Select	0	
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, .PPT etc.	10	Select	0	
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	Select	0	
4	The solution is capable of assigning specific roles for monitoring of role-based document usage.	10	Select	0	
5	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	Select	0	
6	The solution does not have any dependency on software from other vendor for its working.	10	Select	0	
7	The Solution is having integration capability with DLP (Data Loss Prevention) solution and able to apply Keyword based / File Classification based document protection.	10	Select	0	
8	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	Select	0	
9	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	Select	0	
10	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	Select	0	
11	The solution is capable of allowing/ restricting Use/ access of documents, files by users, work groups, devices, IP etc.	10	Select	0	
12	Having capability to modify/revoke the document access post distribution, irrespective of the location of the document.	10	Select	0	
13	Having provision to add/delete users/policy on existing protected files which is already been shared.	10	Select	0	
14	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	Select	0	
15	The solution is having document protection capability on various devices i.e. desktops, laptops, tablets, iOS mobile devices fileservers and Android Mobile.	10	Select	0	
16	The solution is having capability of providing users (Internal/External) rights to access protected documents/ attachments using Android Mobile, IOS Mobile, and Browser.	10	Select	0	
17	View and Edit access to protected information is available on Desktops/Laptop browsers.	10	Select	0	
18	The solution provider is able to provide User Rights template with complete particulars.	10	Select	0	
19	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	Select	0	
20	Solution should have workspace or with bidder provided workspace solution to share the files outside the organization without any dependency on the Email solution and shared drive being used by the Bank All the Tools, Licenses and Workspace have to be factored by bidder from Day 1.	10	Select	0	
21	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	Select	0	
22	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	Select	0	
23	The solution is capable of supporting segregation of duties, defining and assigning different user classes' i.e. End users, system administrators, policy administrators.	10	Select	0	
24	The solution is capable to support delegation of duties and administrative functions for efficient management.	10	Select	0	
25	The solution is able to distinctly handle external and internal users preferably through different user's directory.	10	Select	0	
26	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	Select	0	
27	The external user is able to work i.e., READ and EDIT IRM protected documents as per the rights assigned by document owner.	10	Select	0	
28	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	Select	0	
29	The solution does not require additional licenses for recipients of documents within or outside of the enterprise.	10	Select	0	
30	The solution shall automatically preserve a real-time, immutable and cryptographically verifiable copy of every document protected by the solution and their subsequent versions, either natively or through seamless integration with an bidder proposed on-premise repository solution. The solution shall maintain complete version history, bank-defined retention policies, and a tamper-evident audit trail to ensure document authenticity, integrity and chain of custody for audit, regulatory, legal and forensic purposes.	10	Select	0	
31	The solution is having capability to allow anyone to request access to a file directly from the file owner without any intermediary.	10	Select	0	
32	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	Select	0	
33	The solution is supporting Virtualized environment for deploying server components.	10	Select	0	
34	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	Select	0	
35	The solution allows document creators to assign different rights for each user or group in the same window.	10	Select	0	
36	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	Select	0	
37	The solution can enforce watermarked viewing of protected files even when the files open in native application.	10	Select	0	

38	The solution can define and allocate roles & policies at System Administrator level. Document owner/Administrator should also be able to transfer document rights.	10	Select	0	
39	Solution is providing basic troubleshooting capabilities at user machine that can be easily run by end users themselves.	10	Select	0	
40	The solution shall support secure external sharing of protected documents through a secure link mechanism. The solution shall provide this capability either through native functionality or seamless integration with proposed repository ensuring that protected documents remain under the bank administrative control throughout the sharing lifecycle. The solution shall enforce strict authentication and authorization before granting access to any shared protected document, including time-bound access, revocation, and policy enforcement for shared documents.	10	Select	0	
41	The solution provides off-line use of protected documents; can also control the period for which the user can have offline use.	10	Select	0	
42	The endpoint client/agent should be easy to install and should provide for offline access to protected documents.	10	Select	0	
43	The solution should support installation of endpoint client via standard desktop/infrastructure management tools.	10	Select	0	
44	The solution should have capability of providing documents/ information security irrespective of vendor's/external users computing environment (Storage, Network Connectivity).	10	Select	0	
45	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	Select	0	
46	The solution shall support automated folder-based protection for files stored on central file servers or banks-approved repositories. The solution shall automatically apply protection policies to files based on existing data classification labels or other bank-defined labels, without requiring user intervention. The solution shall continuously monitor designated folders and automatically apply or update protection policies for newly created, modified, or reclassified files	10	Select	0	
47	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	Select	0	
48	The solution is capable of providing protected document recovery in case of cyber-attacks (ransom ware etc.) either through an inbuilt feature or Bidder should provide a 3rd party solution where the DRM protected documents would be stored centrally and recovery in case of cyber-attacks (ransom ware etc.)	10	Select	0	
49	The solution is capable to provide end user the last updated protected documents as per owner directions.	10	Select	0	
50	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	Select	0	
51	The solution should be such that there is no single point for unprotecting the documents other the document owner.	10	Select	0	
52	The solution can support one or more methods applied on data such as password protection, auto-expiry, Geo/IP Fencing, Group policy to ensure greater control over sensitive data.	10	Select	0	
53	The solution is capable of establishing communication within the system as well as with external systems over secured communication protocols like https.	10	Select	0	
54	The solution can allow authenticated users (external) to access (View/Print) protected documents with/without deploying agent	10	Select	0	
B Application Architecture					
55	The architecture should support online real time updation between the application & database	10	Select	0	
56	Integrity of the data should be maintained between the application & database.	10	Select	0	
57	Proposed solution to provide SSO for login in to application & admin modules.	10	Select	0	
58	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	Select	0	
59	Capable of being implemented on a Centralized, localized and / or a hub and spoke model implementation	10	Select	0	
60	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	Select	0	
61	Solution architecture has the capability to be configured in active-active mode	10	Select	0	
62	Application supports database and OS level clustering	10	Select	0	
C Database Requirements					
63	Ability to support for pooling multiple database connections when the load on the application increases	10	Select	0	
64	Ability of the database to support clustering. Indicate the number of clusters that can be configured.	10	Select	0	
65	Ability of the database to support central storage of data with multiple instances of the database	10	Select	0	
66	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	Select	0	
67	Ability to support online replication between DC, DR & NDR.	10	Select	0	
68	Ability to implement SAN's for data storage in the architecture	10	Select	0	
D Hardware and Operating system					
69	The proposed Operating system should support IPV4 & IPV6	10	Select	0	
70	Should be able to support different protocols (HTTP, HTTPS, TCP/IP, TLS, IPX, etc.)	10	Select	0	
E Security / Data Integrity					
71	Integrity of data to be maintained at 100% of time	10	Select	0	
72	Encryption to be used for data traveling between other interfaces	10	Select	0	
73	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	Select	0	
74	sensitive data such as passwords and authentication credentials shall not be logged in transaction or system activity files	10	Select	0	
75	The maximum data length for logging is pre-determined	10	Select	0	
76	Successful and unsuccessful authorization events are logged	10	Select	0	

77	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	Select	0	
78	Sensitive information that is passed in the cookies is encrypted.	10	Select	0	
79	The session identifier shall be random and unique.	10	Select	0	
80	The session shall expire after a pre-defined length of time.	10	Select	0	
81	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	Select	0	
82	The Service Provider shall only install or use cryptographic modules based on authoritative standards and reputable protocols. 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	Select	0	
83	Security framework is supported in terms of authentication, multi-level authorization, auto log-off, password control, single sign-on audit	10	Select	0	
84	System allows administrators to implement access management in a granular manner	10	Select	0	
85	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	Select	0	
86	Activities executed by the Application system administrator.	10	Select	0	
87	Segregation of duties is permitted (e.g. segregated function between system and application administration)	10	Select	0	
88	Ability to define groups so that access can be categorized	10	Select	0	
F	Interfaces				
89	The system should be able to interface with Office365 & Outlook online and seamlessly.	10	Select	0	
90	The system should be able to interface with MS Teams.	10	Select	0	
91	The system should be able to interface with SharePoint.	10	Select	0	
92	The system should be able to interface with OneDrive.	10	Select	0	
93	Application to support various formats not limited to .pdf, .doc, .docx, .xls, .xlsx, .csv, .rif, .ppt, .eml & etc in applying security controls.	10	Select	0	
94	The system should be integrated with DLP system of Bank.	10	Select	0	
95	Interface able to handle exceptions (e.g. will output to log files, retries) when unsuccessful. Able to handle continual processing or gracefully terminated.	10	Select	0	
G	Audit Trail				
96	Does the system provides comprehensive audit trail features such as:				
96.1	Daily activities log are merged into the history log files	10	Select	0	
96.2	Date, time and user-stamped transaction list are generated for different transactions	10	Select	0	
96.3	Do transaction screens display system information including Processing Date, Current Time, Current User	10	Select	0	
96.4	Daily activity reports are provided to highlight all the transactions being processed during the day	10	Select	0	
96.5	Support for recording of Unsuccessful attempts to log-in to the system	10	Select	0	
96.6	System to provide session log files. The user should be able to analyze the information (e.g., account id, session time etc.)	10	Select	0	
96.7	System should provide tracking of the client's IP & Network Interface address	10	Select	0	
H	Reporting				
97	Provide a full set of operational and audit trail reports for each of the modules.	10	Select	0	
98	Periodical reports to appropriate authorities can be generated. The frequency and content of the reports can be determined by the bank user.	10	Select	0	
99	63 Generation / transmission of email alerts / advices at various stages of the transaction	10	Select	0	
100	Support for online access of reports	10	Select	0	
101	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	Select	0	
102	Automatic report generation capability	10	Select	0	
103	Pre-built query feature for non-programmers	10	Select	0	
I	Archival and Restoration				
104	Application should capable to archive and retrieval of history transaction.	10	Select	0	
105	Application should capable to purge the history transaction.	10	Select	0	
106	Purging & Archival should be automated process based on configuration at system/application level.	10	Select	0	
Total		1120		0	

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)	Calculated Score	Remarks
1	Mobile App Security SDK to prevent the mobile app from running on Emulators & Simulators	10	Select	0	
2	Mobile App Security SDK to detect if the mobile app is running on a Jailbroken (for iOS) or Rooted (for Android) device	10	Select	0	
3	Mobile App Security SDK to detect Elevation of Privileges by the attacker	10	Select	0	
4	Mobile App Security SDK to detect if the mobile app is running on an outdated operating system	10	Select	0	
5	Mobile App Security SDK to identify if an android device has third party app store access enabled	10	Select	0	
6	Mobile App Security SDK to detect if USB Debugging Mode and/or Developer Options are enabled on the android device	10	Select	0	
7	Mobile App Security SDK to detect Hooking Frameworks on Devices	10	Select	0	
8	Mobile App Security SDK to detect Device Screen Lock enablement	10	Select	0	
9	Mobile App Security SDK to enforce Device Policy as per business needs	10	Select	0	
10	Mobile App Security SDK to detect if the mobile app is running in a Sandbox environment	10	Select	0	
11	Mobile App Security SDK to detect if the mobile app is launched with the secondary profile on the Android device	10	Select	0	
12	Mobile App Security SDK to detect if mock location settings are enabled on the device	10	Select	0	
13	Mobile App Security SDK to detect time manipulation settings on the device	10	Select	0	
14	Mobile App Security SDK to prevent keystroke recording by malicious apps or keyloggers	10	Select	0	
15	Mobile App Security SDK to detect code injection attempts within the mobile application	10	Select	0	
16	Mobile App Security SDK to implement behavioral-based blacklisting of malicious devices	10	Select	0	
17	Mobile App Security SDK to detect if the mobile app is running on an unsecure Wi-Fi network	10	Select	0	
18	Mobile App Security SDK to identify a Rogue Access Point (RAP) when it is connected to the device	10	Select	0	
19	Mobile App Security SDK to detect MiTM attacks	10	Select	0	
20	Mobile App Security SDK to monitor and prevent SSL Stripping	10	Select	0	
21	Mobile App Security SDK to detect fake certificates used for SSL decryption	10	Select	0	
22	Network threat detection function should be able to work without internet connectivity to app hosting servers	10	Select	0	
23	Mobile App Security SDK to detect Proxy & VPN connections	10	Select	0	
24	Mobile App Security SDK to allow IP whitelisting for trusted VPN connections	10	Select	0	
25	Mobile App Security SDK to detect and defend against offline attacks by identifying when the device has no internet connection	10	Select	0	
26	Mobile App Security SDK to prevent reverse engineering of the mobile app	10	Select	0	
27	Mobile App Security SDK to detect if the mobile app is being tampered	10	Select	0	
28	Mobile App Security SDK to prevent the attackers from decoding or modifying the business logic	10	Select	0	
29	Mobile App Security SDK to detect runtime recompilation or modification of an application	10	Select	0	
30	Mobile App Security SDK to detect if the App is not downloaded from trusted source - Play store and App Store	10	Select	0	
31	Mobile App Security SDK to detect if the App is in Debug Mode	10	Select	0	
32	Mobile App Security SDK to detect if any blacklisted application is present on the mobile device	10	Select	0	
33	Mobile App Security SDK to prevent Screen shot capturing	10	Select	0	
34	Mobile App Security SDK to prevent APK file Decompilation	10	Select	0	
35	Mobile App Security SDK to detect active screen mirroring during App usage	10	Select	0	
36	Mobile App Security SDK to detect App Spoofing Attacks when the App is launched	10	Select	0	
37	Mobile App Security SDK to detect side loading when the mobile app is launched	10	Select	0	
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 behaviour methodology and not on signature methodology	10	Select	0	
39	Mobile App Security SDK to identify any overlay during App usage	10	Select	0	
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	Select	0	
41	Mobile App Security SDK to prevent Picture-in-Picture (PIP) Attacks and Draw over other App	10	Select	0	
42	Mobile App Security SDK to identify Admin & Accessibility permission for Sideloaded Apps	10	Select	0	
43	Mobile App Security SDK should comply with RBI DPSC guidelines	10	Select	0	
44	Mobile App Security SDK should comply with OWASP Mobile Top 10	10	Select	0	
45	Mobile App Security SDK should be able to support any device model having minimum Android version 8 or iOS version 12	10	Select	0	

46	Mobile App Security SDK to notify the host application through callbacks in the event of device, network or malware-based threat detection	10	Select	0	
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	Select	0	
48	Mobile App Security SDK should not collect any PII data from device or app	10	Select	0	
49	Mobile App Security SDK should be able to allow for the usage of custom device identifiers and labels	10	Select	0	
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	Select	0	
51	Mobile App Security SDK to support React Native framework	10	Select	0	
52	Mobile App Security SDK should provide the means of mapping the threat data detected with the actual user session or user id	10	Select	0	
53	Mobile App Security SDK should comply with the security policies of Play Store and App Store, etc.	10	Select	0	
54	Management Console Should integrate with SIEM/SOC platforms and provide all detailed threat forensic information	10	Select	0	
55	Management Console should integrate with Fraud Prevention System	10	Select	0	
56	Management Console should support Rest API's for integration with backend system	10	Select	0	
57	Mobile App Security SDK to provide unique ref. or message ID on detection of each threat	10	Select	0	
58	Mobile App Security SDK should have the capability to collect information of applications and processes running at the time of threat detection	10	Select	0	
59	Mobile App RASP solution must be SDK based and there should not be dependency on Service provider for App version upgrades	10	Select	0	
60	System Control Portal should be a web-based solution for configuration, integration and reporting of Mobile App RASP Solution	10	Select	0	
61	System Control Portal should provide Role based access to console with proper segregation of group of users and functions.	10	Select	0	
62	System Control Portal should provide details of No. of devices on which App is running on with breakup of Android and iOS devices.	10	Select	0	
63	System Control Portal should include details such as device OS version details, OS level threats detected, etc.	10	Select	0	
64	System Control Portal should provide customizable Threat Policy configuration for different Apps	10	Select	0	
65	System Control Portal should provide over the air updates for rule upgrades and configuration	10	Select	0	
66	System Control Portal should provide statistics on Daily, Monthly Active devices	10	Select	0	
67	System Control Portal should provide Dashboards highlighting change in trend of threats	10	Select	0	
68	Service Provider should provide quarterly version updates	10	Select	0	
69	Service provider should assist to close any code related vulnerabilities identified during VAPT or Code Review	10	Select	0	
70	Service provider should undertake detailed Threat Modelling exercise before implementation of Mobile RASP solution	10	Select	0	
Total		700		0	

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

HIPS & Workload protection					
S.No	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The solution should offer a comprehensive server and workload protection capabilities against known and unknown threats.	10	Select	0	
2	Solution should have all protection modules like Anti-Malware, Deep Packet Inspection with HIPS, Host-based Firewall, Integrity Monitoring, Application Control, Device Control, OS Log inspection, Memory Protection capabilities in a single agent.	10	Select	0	
3	The proposed server security solution must support multiple platforms of server operating systems i.e. AIX, Alma Linux, Amazon Linux, CentOS, Cloud Linux, Debian Linux, Miracle Linux, Oracle Linux, RHEL, RedHat OpenShift, Rocky Linux, Solaris, Suse, Ubuntu, Windows, Docker, Docker CE, Docker EE.	10	Select	0	
4	Solution should be deployed on-premises and should also have provision to configure agent Relays that will assist in optimizing the update distribution and reduces the load on HIPS & Anti-Malware manager	10	Select	0	
5	The solution must detect and protect against:	-			
5.1	All kinds of viruses, Trojans, worms, rootkits, backdoors, network viruses, spyware, keyloggers, hacking tools, greywares including but not limited to master boot sector, memory resident, macro, polymorphic malware, ransomware, web-based threats, network-based attacks and any other forms of exploits	10	Select	0	
5.2	Vulnerability and exploit attacks, with deep instrumentation of web frameworks at http/https as well as underlying layer like middleware, and databases	10	Select	0	
5.3	Network attacks such as reconnaissance/DOS, undefined lateral movement, peer-to-peer communication, etc.	10	Select	0	
6	The solution should have multiple scanning techniques like Machine learning and behavior analysis to detect and prevent advanced threats like unknown and zero-day threats on the servers.	10	Select	0	
7	Machine learning must have both Pre-execution intelligence of extracting file features and run-time analysis of file/process behavior to identify threats.	10	Select	0	
8	The solution should have multiple scan configuration to allow admin to perform in real time, demand scan, manual scan, schedule scan at preferred time window, and configurable through the GUI. There should be a defined mechanism to whitelist the file / directory from real time scan.	10	Select	0	
9	The solution must be able to create copies of files being encrypted by a ransomware on the server and it must be able to restore the affected files back to their original state.	10	Select	0	
10	The solution must be able to identify communication over HTTP/HTTPS protocols and commonly used HTTP ports, it must be able to detect/prevent communications to Global C&C's and Allow administrators to create user defined list also.	10	Select	0	
11	The solution must provide application of customized enforcement actions based on malicious file types such as Delete, Terminate/Block, Quarantine.	10	Select	0	
12	The solution should provide automated recommendations and enforcement of protection policies against known vulnerabilities. It must support automatic removal or adjustment of protection rules when vulnerabilities are resolved, such as disassociating outdated signatures after patches are applied. The scheduling of these actions should be configurable by administrators with flexible options like hourly, daily, weekly, or monthly intervals.	10	Select	0	
13	The solution shall detect RCE vulnerabilities and provide complete visibility of detected vulnerabilities in servers with CVE details. The proposed solution should automatically assign the interim compensatory rules/filters on the servers to shield against the detected RCE vulnerabilities.	10	Select	0	
14	Firewall rules should filter traffic based on source and destination IP address, Port, MAC address, etc. and should detect reconnaissance activities such as port scans. Solution should be capable of blocking and detecting IPv6 based attacks.	10	Select	0	
15	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support creation of custom rules as well.	10	Select	0	
16	The suggested solution should utilize a baseline secure state as a benchmark, conduct scans for unforeseen alterations to registry values, registry keys, services, processes, installed software, ports, and files. It should then log an event and, optionally, trigger an alert upon detecting any unexpected changes.	10	Select	0	
17	The application whitelist/control model should also be able to control what processes, libraries or scripts are allowed to run and further their runtime behavior.	10	Select	0	
18	Solution shall have the ability to detect applications that attempt to spread themselves over the network, it shall inspect applications, as well as the applications' sub-components (DLLs) as they are executed.	10	Select	0	
19	Solution should have an intuitive rule creation and modification interface includes the ability to include or exclude files using wildcards filenames, control over inspection of sub-directories.	10	Select	0	
20	Solution should have client-server architecture model to manage the agents, their security policies and log management from a single console. There should be an option to provision relay servers to optimize the bandwidth utilization, if applicable.	10	Select	0	
21	For secure communication between agent and management server, the management server must allow 3 rd party certificate import.	10	Select	0	

22	Solution should be able to work with Integrated threat protection wherein solution should be able to share the suspicious objects/detected IOCs for the unknown threats which are analyzed in sandboxed environment	10	Select	0	
23	The solution shall provide submission of suspicious files to a sandbox / threat- analysis solution for virtual execution / Root-Cause analysis. The sandbox / threat - analysis solution shall provide execution / RCA result for the suspicious file.	10	Select	0	
24	The solution incorporates real-time integrity monitoring, actively scanning critical operating system and application elements such as directories, files, registry keys, and values. It promptly detects and reports any suspicious activity, particularly unauthorized modifications. Furthermore, the solution empowers users to create manual rules, enhancing the effectiveness of the integrity monitoring process.	10	Select	0	
25	The solution should include a Log Inspection module capable of capturing and analyzing system logs, providing audit evidence to meet PCI DSS or internal requirements within your organization. Additionally, the solution should have the ability to forward suspicious events to an SIEM system or centralized logging server for correlation, reporting, and archiving purposes.	10	Select	0	
26	The solution should possess Common Criteria EAL 2+ and FIPS 140-2 validation, ensuring compliance with rigorous security standards.	10	Select	0	
27	The solution should support DDOS protection rules as a part of HIPS capabilities	10	Select	0	
28	Solution should have device control capabilities to allow/block USB on Windows Servers/Vms	10	Select	0	
29	The solution should have the capabilities to detect reconnaissance scans on server/VMs	10	Select	0	
30	The Solution should support agent version control, to ensure "n", "n-1", "n-2" agent version can be deployed as per the process laid by PSB	10	Select	0	
31	Solution should support ant-tampering of agent for both windows and Linux based operating systems	10	Select	0	
32	Solution should offer customizable dashboard to view computer status, alert status, total sign-ins, anti-malware events, integrity monitoring events, firewall events etc.	10	Select	0	
33	Grouping / sub-grouping of servers/VMs should be possible for ease of management on the console	10	Select	0	
34	Solution should provide out of the box report both on the console as well as over email in CSV, PDF and RTF format	10	Select	0	
35	Solution should also offer protection from polymorphic attacks	10	Select	0	
Total		370		0	

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

WAF					
S.No	Functional Specification	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The proposed solution should provide different level of user accounts, permissions, and access levels for managing the WAF.	10	Select	0	
2	The OEM Should provide timely updates of attack signatures and patterns to detect and prevent new threats. The immediate support like log4J vulnerability should be supported immediately	10	Select	0	
3	The proposed solution should have native feature of generating comprehensive reports on WAF performance, security events, and incidents.	10	Select	0	
4	The proposed solution should provide flexibility to build customize report template	10	Select	0	
5	Should have to access to appliance via the following: a) Web Based Management (WBM), using HTTPS. b) Command Line Interface (CLI), via SSH, or Console access. c) REST API over HTTPS	10	Select	0	
6	Should have centralized management application, and complete configuration of appliance	10	Select	0	
7	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	Select	0	
8	The Solution should have system-wide rate limiting command.	10	Select	0	
9	Conduct scheduled failover tests to ensure seamless failover in case of primary device failure.	10	Select	0	
10	Should have VRRP based Failover or other proprietary failover mechanisms	10	Select	0	
11	The proposed solution should have the capability to perform regular backups and restore configurations when needed.	10	Select	0	
12	The proposed solution must support dedicated 5 Gbps of WAF throughput (HTTP/HTTPS). The bidder must provide evidence of throughput through publicly available documents /evidence based document supporting the same which needs to be submitted along with the proposal and same needs to showcased if asked by bank during Presentation & UAT (Undertaking from the OEM is not accepted in this case).	10	Select	0	
13	The solution must be appliance-based rack mountable and must be available as Physical appliance.	10	Select	0	
14	The Proposed WAF should support minimum 30000 RSA Per SEC (2048 BIT) & 10000 TPS with ECC and < 5ms latency	10	Select	0	
15	The Proposed WAF should have dual hot swapable power supply as per India Standard from day one	10	Select	0	
16	The Proposed WAF must support the following deployment modes to monitor web application traffic over the network: It must support both HTTP and HTTPS for all the following modes. Depending on the requirements and use cases Bank may decide to use any of the mode. - Layer-2 inline bridge mode - Layer 3 Reverse Proxy mode	10	Select	0	
17	All the WAF appliance must be centrally managed. It must provide the following capabilities: - Unified management and administration of federated environments across all WAF - Creation, configuration and distribution of policies system-wide across all WAF - Single point of access to each WAF appliance - Monitoring of solution health for the entire deployment - System wide view of security activities	10	Select	0	
18	The solution must support the positive security model approach. A positive security model states what input and behavior is allowed and everything else that deviates from the positive security model is alerted and/or blocked.	10	Select	0	
19	The solution must support the negative security model approach. A negative security model explicitly defines known attack signatures.	10	Select	0	
20	The solution must be able to execute the following actions upon detecting an attack or any other unauthorized activity: - Ability to drop requests and responses, - Block the TCP session, - Block the application user - Block the IP address	10	Select	0	
21	The solution must be able to block the user or the IP address for a configurable period of time.	10	Select	0	
22	The solution must be able to protect both HTTP Web applications and SSL (HTTPS) web applications.	10	Select	0	
23	The solution must be able to inspect and protect both HTTP/1.x , HTTP/2 and HTTP/3(Should support in future) protocols.	10	Select	0	
24	The solution must be able to reencrypt SSL web traffic between WAF and web servers.	10	Select	0	
25	The solution must provide the following features and protection. - Web service layer correlated attack validation - HTTP protocol attack signatures - Web service layer customized protection - Cookie signing validation - Web profile protection - Web application attack signatures - Web application layer customized protection - OCSP protocol validation	10	Select	0	
26	The solution must support the custom signatures definitions	10	Select	0	

27	The solution must support regular expressions for the following purposes: - Signatures definition - Sensitive data definition - Parameter type definition - Host names and URL prefixes definition	10	Select	0	
28	The solution must support automatic updates to the signature database to ensure complete protection against the latest web application threats.	10	Select	0	
29	The solution must have a correlation engine built-in to provide event correlation and automated baselining.	10	Select	0	
30	The solution's in-built correlation engine must address complex attacks that are ambiguous in nature. It must also examine multiple pieces of information at the network, protocol and application levels over time to distinguish between attacks and valid user traffic.	10	Select	0	
31	The solution must be able to detect known malicious users who are often responsible for automated and botnet attacks. The source of malicious users include malicious IP addresses, anonymous proxy addresses, and TOR networks.	10	Select	0	
32	The solution must be able to identify WebSocket connections.	10	Select	0	
33	The solution must be able to perform validation on all types of input, including URLs, forms, cookies, query strings, hidden fields, and parameters, HTTP methods, XML elements and SOAP actions.	10	Select	0	
34	The solution must be capable of automatically perform dynamic profiling of web applications.	10	Select	0	
35	The solution dynamic profiling technology must be able to detect and protect against threats which are specific to the custom code of the web application. After the dynamic profiling/learning phase, the solution must be able to understand the structure of each protected URL.	10	Select	0	
36	The solution must automatically build/learn the web application profiles and use them to detect deviations and various anomalies (or violations) and block attacks on the custom code of the application.	10	Select	0	
37	The solution must be able to automatically learn the web usage and application structure and elements and expected user behaviors as soon as the system is installed. The structure and elements include URLs, directories, cookies, form fields and parameters, and HTTP methods.	10	Select	0	
38	The solution must allow the re-learning of an application profile on a per-URL or per-page basis. The administrator should not be required to relearn the entire application when only a few pages have changed.	10	Select	0	
39	The solution must support the configuration to allow some pages in a web application to be in protected mode and some pages to be in dynamic profiling learning mode.	10	Select	0	
40	The solution must be able to perform dynamic profiling of JSON/XML. HTTP requests in the JSON format must be learnt by the WAF with the parameters and values.	10	Select	0	
41	The solution must be able to protect web applications that include Web services (API) content.	10	Select	0	
42	The API protection offered by the solution must be similar to the web application protection provided with automated dynamic profiling/learning capability.	10	Select	0	
43	The solution should integrate with web application vulnerability assessment tools (Web application scanners) to virtually patch web application vulnerabilities.	10	Select	0	
44	The solution must address and mitigate the OWASP Top Ten web application security vulnerabilities.	10	Select	0	
45	The solution must be able to provide a OEM threat intelligence service based on source reputation. The Cost is to be part of the BOM, no additional cost shall be payable to the bidder/OEM The feed must be provided in near-real time for the following known attack sources: - Malicious IP - Anonymous Proxies - TOR IPs - Geo Location	10	Select	0	
46	The solution must have the capability to provide threat intelligence emergency feeds service. This service shall provide the latest set of signatures from the solution vendor to mitigate zero-day vulnerabilities as soon as they are identified.	10	Select	0	
47	The solution must be able to prevent automated layer 7 DDoS Attack, web scraping and brute force attack being directed to the site	10	Select	0	
48	The solution must provide "anti-automation" protection which can block the automated attacks using hacking tools, scripts, frame work etc.	10	Select	0	
49	The solution must support masking of sensitive data in alerts.	10	Select	0	
50	The solution should integrate with SIEM & SOC- Big Data Lake for sending all type of alerts.	10	Select	0	
51	Solution must be integrated with SIEM or other log collection server.	10	Select	0	
52	The solution must support the creation of custom log messages	10	Select	0	
53	The solution must support a flexible set of follow-up actions to be taken in the event of an alert generation.	10	Select	0	
54	The solution must provide functionality to assist with security event forensics/Analysis.	10	Select	0	
55	The solution must have the functionality that enables the administrator to create custom report templates	10	Select	0	
56	The solution must support generation of reports with both tabular views and data analysis graphical views.	10	Select	0	
57	The solution must support automatic generation of reports based on a defined schedule.	10	Select	0	
58	The solution must come with a web based administration interface and GUI.	10	Select	0	
59	The solution management appliance must support centralized management and reporting for proposed WAF appliances at both DC & DR.	10	Select	0	
60	The solution on-premise management solution must be able to manage a WAF appliance that is deployed on-premise.	10	Select	0	
61	The OEM should have Support Centers / Service Center in India with 24x7x365 TAC support.	10	Select	0	
62	The proposed WAF solution should be enabled with all the modules and features from day one without any additional license dependency.	10	Select	0	

63	All the custom policy and signature creation must be done via GUI. There should not be any need to create any advanced policy from CLI.	10	Select	0	
64	The solution must have a GUI based option to create policies to detect and block Double encoding attacks.	10	Select	0	
65	The WAF solution must have AI/ML based Analytics that would correlate and distill thousands of security events into a few distinct readable events.	10	Select	0	
66	The vendor is responsible to ensure that the solutions and operations comply with information security policies and industry leading standards (such as ISO 27001, etc.) and any applicable laws and regulations (such as RBI, DPDP Act etc.).	10	Select	0	
67	The proposed solution should not have restrictions on number of rules	10	Select	0	
68	Proposed solution should be able to detect and block the latest OWASP top 10 and OWASP Top 10 API	10	Select	0	
69	Should be able to provide PCI DSS compliance and reporting	10	Select	0	
70	System should protect against the following threats: • SQL injection • Cross-site scripting (XSS) • Cross-Site-Request-Forgery (CSRF) • Parameter tampering • Hidden-field manipulation • Session manipulation • Cookie poisoning • Cookie protection • Remote file inclusion • Buffer overflow • Stealth commanding • Backdoor and debug options • Application-buffer-overflow attacks • Brute-force attacks • Data encoding • Unauthorized navigation • SOAP- and Web-services manipulation • Web Scraping	10	Select	0	
71	System supports enforcing policies regardless of character encoding in order to combat evasion techniques, such as: • URL-decoding (for example, %XX) • Self-referencing paths (that is., use of ../ and encoded equivalents) • Path back-references (that is, use of ../ and encoded equivalents) • Mixed case • Comment removal (for example, convert DELETE/**/FROM to DELETE FROM) • Conversion of (Windows-supported) backslash characters into forward slash characters. • Conversion of IIS-specific Unicode encoding (%uXXYY) • Virtual directory route—positive folder enforcement • Base64 Encoding	10	Select	0	
72	Device should able to control BOT traffic and It should able to block known bad bots and fake search engine requests	10	Select	0	
73	Should support XML Application protection	10	Select	0	
74	The solution should provide full support for HTML5, AJAX and JSON.	10	Select	0	
75	Should have Geo-IP Blocking capability	10	Select	0	
76	Solution should be able to provide User Defined Customized Reporting	10	Select	0	
77	The solution should be able to block even the most advanced bots that try to emulate standard client behavior and pretend to be web browsers.	10	Select	0	
78	The solution must protect against common risks from automated traffic, including: - Scraping – unauthorized content extraction - Spamming – mass data submissions - Screwing – manipulation of analytics and statistics - DDoS – application overload attacks - Denial of Inventory – bulk carting to block real users - Carding/Card Cracking – payment card fraud attempts	10	Select	0	
79	Client Identification and Behavioral Analysis Requirement: The solution must support client identification by injecting JavaScript into the browser to collect detailed runtime environment data	10	Select	0	
80	The client component (JavaScript) should be resistant to reverse-engineering techniques through advanced code obfuscation techniques and frequent script changes	10	Select	0	
81	The client component (JavaScript) should be downloaded from the same domain as the application (first party). It is not allowed to use external locations to upload the script.	10	Select	0	

82	Identification should be implemented with the accuracy of the web browser. The result of the identification should be the establishment of a session with the browser, which will authorize further communication.	10	Select	0	
83	The solution should allow the definition of specific endpoints which are crucial for the application, which will be accessible only after previous identification and application of policies. Sending a request to such an endpoint without prior identification should result in immediate block of the request and redirecting the client to the website which will initiate the identification.	10	Select	0	
84	The solution must include machine-learning or behavioral analysis mechanisms. They should detect anomalies in the behavior of application clients and classify bots based on similar behavioral patterns.	10	Select	0	
85	The solution should also provide protection for APIs that are consumed by browsers. Interfaces can then be accessible depending on the presence of a valid session key assigned at identification time.	10	Select	0	
86	The system should provide the ability to apply the following actions against traffic classified as BOT: · blocking · monitoring · displaying a captcha	10	Select	0	
87	The manufacturer should manage some of the conditions (lists) that can be easily placed in the policy, including: · Social Media Bots · Search Engines bots · Aggregator User Agents · CSPs (expected lack of client traffic)	10	Select	0	
88	The system should have a number of predefined conditions/rules that are most commonly used. It should also be possible to freely define conditions based on logical operators and analysis of attributes acquired during identification.	10	Select	0	
89	Part of the product should be a flexible reporting system that can generate detailed views, including: · Applied actions on the timeline · Number of solved/unsolved captcha · The performance of ML models · The incidence of customer anomalies · Ratio of bad bot/good bot/human traffic · Endpoints with the highest number of requests.	10	Select	0	
90	The proposed WAF solution must support high availability in both Layer 2 and Layer 3 deployments. It must include either an inbuilt bypass switch or be supplied with an external bypass switch to ensure uninterrupted traffic flow during maintenance or failure.	10	Select	0	
91	The appliance must be a purpose built WAF with its own custom specialized hardened OS integrated with the proposed hardware.	10	Select	0	
92	The solution must have bypass segments to ensure that fail open in case of hardware failure	10	Select	0	
93	The WAF shall use advanced Machine Learning (ML) algorithm to automatically learn application behavior, including URL/URI structure, application flow, parameter schema, data types, and request patterns to detect anomalies	10	Select	0	
94	The proposed solution shall support PQC readiness, including support for secure cryptographic mechanisms and standards that facilitate future migration to quantum-resistant cryptography, wherever applicable to the solution.				
95	The solution shall provide built-in Vulnerability Assessment to identify web application vulnerabilities, with the WAF automatically enforcing Virtual Patching policies to protect applications without requiring application code changes. As per the guidelines by Govt Body.	10	Select	0	
96	The WAF solution should be capable to store all logs for at least one month on appliance itself. Bidder to ensure that bidder right size the same. Bidder to submit the detailed calculation of Hard Disk and RAM requirement to meet the bank RFP ask of storage on-appliance and Response along with any bottleneck mitigation and SLA compliance. If any stage the same is observed bidder is required to provide the additional hardware/component to mitigate the same at no additional cost to the bank	10	Select	0	
Total		950		0	

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

Centralized Key management Solution (KMS)					
S. No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The Virtual form-factor of KMS should be FIPS certified (with certification in the name of the OEM)	10	Select	0	
2	The system should support an easy way to centrally store and manage key & secret lifecycle tasks	10	Select	0	
3	The system should support AES(128-256), ARIA,ECC(224-512), Brainpool curves, HMAC , TDES, RSA(512-4096) and the Crypto mode (CBC, CBC-CS1,ECB,GCM) etc.	10	Select	0	
4	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	Select	0	
5	The System shall support Multi-tenancy using multiple domains, Clustering, High Availability and Backup.	10	Select	0	
6	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	Select	0	
7	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	Select	0	
8	Solution should support Multi Factor Authentication (MFA) for users accessing protected path on Windows Servers either through inbuilt feature or integrating with the bank's MFA solution	10	Select	0	
9	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	Select	0	
10	The solution should provide capabilities for key discovery, vulnerability assessment, centralized inventory, key 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	Select	0	
11	The Key Manager should offer various encryption and key discovery tools to locate keys and other secrets in servers , configuration files etc giving a single glass pane view for centralized management.				
12	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	Select	0	
13	The system should be configured to send e-mail notifications to specific addresses when system alarms are triggered.	10	Select	0	
14	The Key Discovery tool should be able to be managed from the KSM console and should be able to discover secrets like AES Key, AWS Key ID, Azure Storage Key, Mailchimp Access Key, Private Key, SendGrid API Key, SSH Private Key, SSH Public Key, Stripe Access Key, TDES Key, Twilio API Key, RSA Key, PGP Key, ECC Keys, Asymmetric Keys etc.	10	Select	0	
15	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 in order to maintain the complete ownership	10	Select	0	
16	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	Select	0	
17	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	Select	0	
18	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	Select	0	
19	The Solution supports capability to protect data through encryption or tokenization using a FIPS 140-2 level 3 compliant solution.	10	Select	0	
20	Should support administrative interfaces like GUI, REST API, CLI, SNMP v1, v2c, v3, NTP, Syslog-TCP	10	Select	0	
21	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	Select	0	
22	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	Select	0	
23	The Proposed solution should be capable of Ransomware detection and blocking capability	10	Select	0	
24	Network Management - SNMP, NTP, Syslog-TCP.	10	Select	0	
25	The Solution should integrate with SIEM/S-BDL to send the Syslog	10	Select	0	
26	API Support - • REST • KMIP • JCE, .NET, MSCAPI, MS CNG, API's and libraries for integration into custom applications.	10	Select	0	
27	The proposed solution shall support centralized cryptographic key lifecycle management, including secure key generation, storage, backup, distribution, rotation, escrow (where applicable), archival, recovery, revocation, and secure destruction, while enforcing configurable cryptographic policies and segregation of duties.	10	Select	0	
28	The proposed solution shall support industry-standard cryptographic algorithms, key lengths, protocols, and certificate formats in accordance with internationally accepted standards and current industry best practices, and shall support migration to newer cryptographic standards without significant disruption to business operations.	10	Select	0	
29	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	Select	0	

30	The proposed solution shall integrate with standards-compliant Hardware Security Modules (HSMs) through industry-standard interfaces for secure generation, protection, and management of cryptographic keys and execution of cryptographic operations without exposing private keys in plaintext.	10	Select	0	
31	HSM should be able to support : RSA(2048-8192), DSA, Diffie-Hellman, ECC ,ECDSA, ECDH, Ed25519, ECIES (No separate license for algorithm)	10	Select	0	
32	HSM should be able to support :AES, AES-GCM, DES, Triple DES	10	Select	0	
33	Keys must remain securely inside the HSMs FIPS 140-3 Level 3 validated cryptography boundary throughout the key lifecycle	10	Select	0	
34	HSM should support Hash algorithms like : (Hash/Message Digest/HMAC): SHA-1, SHA-2, SHA-3	10	Select	0	
35	HSM should have SP800-38F, SP800-108	10	Select	0	
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	10	Select	0	
37	HSM must support minimum 5 cryptographically isolated partitions per device	10	Select	0	
38	HSM must support the capability to run the custom code inside the HSM	10	Select	0	
39	HSM must support Kyber key generation ,hash-based HSS, XMSS and XMSSMT (Multi-tree), and the Dilithium signing operations PQC algorithms	10	Select	0	
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	Select	0	
41	HSM should have alarm triggers for motion, voltage and temperature	10	Select	0	
42	Security between HSM and the HSM client includes Message authentication	10	Select	0	
43	Connections with HSM Client should terminate on HSM card and not on HSM chassis	10	Select	0	
44	HSM should have FIPS 140-3 Level 3 security certification (with certification in the name of OEM)	10	Select	0	
45	HSM must have CC EAL4+ on same appliance (with certification in the name of OEM)	10	Select	0	
46	HSM must have UL, CE, FCC, CE, RoHS2, India BIS [IS 13252 (Part 1)/IEC 60950-1]	10	Select	0	
47	SNMP, Syslog support and remote management capability	10	Select	0	
48	PKCS#11, Java (JCA/JCE), Microsoft CAPI and CNG, OpenSSL and REST API for administration	10	Select	0	
49	HSM must have containerization to allows granular control of key material for applications requiring high assurance by providing segregation of partition traffic for each applications	10	Select	0	
50	Only permitted IP can initiate SSH access to the HSM appliance	10	Select	0	
51	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	Select	0	
52	The HSM OEM should provide a software-based simulator, virtual HSM, or equivalent development environment to facilitate application integration, testing, and validation. The simulator/virtual HSM/Development environment should support standard HSM interfaces/APIs and enable remote connectivity over the network wherever applicable. Availability of such simulator/ virtual HSM/Development environment shall be provided by the OEM without additional licensing cost to the bank.	10	Select	0	
53	The HSM must support the latest containerized technology that allows multiple independent containerized HSM to run in a single HSM machine. Each containerized HSM is independent and isolated from others, they can be started, stop and upgrade firmware without affecting the rest of containerized HSMs in the machine.	10	Select	0	
54	The HSM shall provide supported Software Development Kit (SDK) and standard cryptographic interfaces/ APIs to enable application integration, cryptographic operations, and development of supported extensions without compromising the security certification of the HSM.	10	Select	0	
55	The HSM shall support secure lifecycle management of cryptographic keys, including backup, restore, replication, and distribution mechanisms for secure management of Post-Quantum Cryptographic algorithms, including stateful algorithms	10	Select	0	
56	The HSMs must be in Secure Transport Mode (STM), to ensure HSM have not been altered while in transit	10	Select	0	
57	HSM should support the backup on FIPS certified hardware device, not to file in any form.	10	Select	0	
Total		560		0	

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

Certificate Lifecycle management solution (CLM)					
S. No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	Certificate Lifecycle management (CLM)				
1	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	Select	0	
2	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	Select	0	
3	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	Select	0	
4	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	Select	0	
5	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	Select	0	
6	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	Select	0	
7	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	Select	0	
8	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	Select	0	
9	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	Select	0	
10	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	Select	0	
11	The proposed solution shall support the complete lifecycle management of digital certificates, including automated discovery, inventory, issuance, enrollment, renewal, deployment, replacement, revocation, expiry monitoring, and secure retirement of certificates, along with configurable alerts, workflow-based approvals, audit trails, and comprehensive reporting.	10	Select	0	
12	Quantum attacks on RSA/ECC encryption - The CLM solution should protect digital certificates, VPNs, and encrypted communications against quantum computers	10	Select	0	
13	Harvest Now, Decrypt Later (HNDL) attacks - The CLM solution should enable rapid migration to quantum-safe cryptography before future decryption becomes possible	10	Select	0	
14	Quantum compromise of PKI- The CLM solution should ensure long-term trust in certificates and digital identities	10	Select	0	
15	Quantum attacks on payment systems- The CLM solution should ensure protection and lifecycle management of certificates securing payment applications payment transactions, RTGS, UPI, and SWIFT communications	10	Select	0	
16	Quantum threats to stored banking data- The CLM solution shall enable protection of customer records and financial archives from future quantum decryption	10	Select	0	
17	Cryptographic asset visibility gaps- The CLM solution should identify vulnerable cryptographic algorithms across enterprise systems	10	Select	0	
Total		170		0	

IDAM					
S. No.	Functional Specifications	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A	Unified Identity Platform				
1	Unified identity platform should include automated identity intelligence, authentication, access, SSO, governance and lifecycle as part of the single unified platform	10	Select	0	
2	Proposed unified platform components (Authentication, SSO and IDAM) should be from a single OEM for seamless integration	10	Select	0	
B	Identity and Access Management (IDAM)				
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	Select	0	
C	Life Cycle Management				
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	Select	0	
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	Select	0	
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	Select	0	
7	Solution must have capability to check duplication of User IDs and not allow creation of duplicate User IDs. (Duplication of user ids)	10	Select	0	
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	Select	0	
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	Select	0	
10	Solution must have capability for configuration of workflow based on joiner, mover or leaver scenarios.	10	Select	0	
11	Solution must have capability for provisioning of users into variety of on-prem. and cloud based business applications	10	Select	0	
12	Solution should provide integration with Finacle(CBS) 10 and above. Bidder to provide the client reference where integration has been done with CBS Finacle 10 and above	10	Select	0	
13	Solution should support modification of user's access based on transfer and promotions.	10	Select	0	
14	Solution must allow users to assign a delegate while away from the office for example, while on vacation. (Delegation of Authority)	10	Select	0	
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	Select	0	
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	Select	0	
17	Solution must allow to create/import user and their roles using manual (ex. csv) and automated interfaces.	10	Select	0	
18	Solution should support a 'least privilege' security model by decentralizing control with delegated administration.	10	Select	0	
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	Select	0	
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	Select	0	
D	User Interface				
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	Select	0	
22	with Visual, event-driven workflow designer for easier visual workflow configuration	10	Select	0	
23	with Localization & Accessibility for Better multi-language, responsive design support	10	Select	0	
24	The same UI should cater to all areas, including roles simulation, workflow design, access request, Policies and application on-boarding	10	Select	0	
E	User Access & Policy Review				
25	Solution must have capability to review and certify user access periodically to ensure that users have the right access.	10	Select	0	
26	Solution must have capability to highlight privileged user accounts and other high-risk accounts (e.g., service accounts, bots) during the certification process	10	Select	0	
27	Solution must provide four different access certification campaign for periodic access review:				
27.1	Entitlement.	10	Select	0	
27.2	Role Certification.	10	Select	0	
27.3	Application/Owner Account.	10	Select	0	

IDAM

27.4	User Identity/Manager Account.	10	Select	0	
28	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	Select	0	
29	Solution must have capability for a multi-step access review process so that more than one reviewer can verify the user access.	10	Select	0	
30	Solution must provide governance administration capabilities integrate tightly with the provisioning solution so that any access that is denied is immediately revoked	10	Select	0	
31	Solution must provide a single policy repository that is leveraged by all identity processes, including both detective and preventive access controls.	10	Select	0	
32	Solution must automatically scan and detect policy violations.	10	Select	0	
33	Solution must have capability to pull & generate reports in different logs format such as pdf and csv.	10	Select	0	
34	Solution should be able to manage segregation of duties in applications.	10	Select	0	
35	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	Select	0	
36	Solution must support the ability to define and enforce access policies, including Separation of Duties (SoD) policies, between individual roles, between individual entitlements.	10	Select	0	
37	Solution must capture all activity information as part of audit logging & forward it to SIEM	10	Select	0	
38	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	Select	0	
F	Access Request				
39	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	Select	0	
40	Solution must have capability to enable the approver (manager, owner, etc.) to approve at a group or fine grained entitlement level.	10	Select	0	
41	Solution must have capability to support end dates for when access should be granted on a temporary basis.	10	Select	0	
42	Solution must support access request end-dates will remove the access whenever the approved time and date is reached.	10	Select	0	
43	Solution must have capability to Automatically provision user access after access has been approved/authorized.	10	Select	0	
44	Solution must have capability to identify users that have been provided access to systems directly by admins instead of by the IDAM solution.	10	Select	0	
45	Solution must provide tools for identifying and managing orphan, rogue accounts	10	Select	0	
46	Solution should have the capability to allow integration with 3rd party solutions via API.	10	Select	0	
G	General Requirement				
47	Solution must run in a virtualized application environment such as VMware	10	Select	0	
48	Solution must support bulk load mechanisms that can be used to quickly load data for users, accounts, services into the IDAM system.	10	Select	0	
49	Proposed solution must be scalable to support future business growth	10	Select	0	
50	Proposed solution must support clustering for load balancing and/or fail-over purposes	10	Select	0	
51	Solution must support policies to enforce rules related to password complexity, expiry, length, password aging, password composition and password history enforcement. (Password policy)	10	Select	0	
52	Solution must have capability for Synchronization of passwords across managed systems. (Password synchronization)	10	Select	0	
53	Solution must integrate with Bank's privileged access management systems	10	Select	0	
54	Solution must integrate with Bank's security information & event management (SIEM) solutions	10	Select	0	
55	Solution must integrate with Bank's mail solution	10	Select	0	
56	Solution must interface with various mechanism to push data into the solution and pull data out of the solution	10	Select	0	
57	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	Select	0	
58	The proposed solution shall provide a configurable connector framework to establish integrations using APIs and SCIM, facilitating rapid integration with enterprise applications for standard use cases. The solution shall also support custom connector development for non-standard integration requirements.	10	Select	0	
H	Self-Service Access Request				
59	Solution must provide self-service interface/module for users for additional access request	10	Select	0	
60	Solution must have capability to allow users to manage their passwords and to reset a forgotten password without the help of an administrator.	10	Select	0	
61	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	Select	0	
I	Reports				
62	Solution must support saving reporting results in downloadable file formats (e.g., PDF, Excel or CSV)	10	Select	0	
63	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	Select	0	

64	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	Select	0	
65	Solution must provide reports on Orphan Accounts and Policy violation	10	Select	0	
J	Provisioning & Connectivity Requirement				
66	Solution must support account/access provisioning	10	Select	0	
67	Solution must provide out-of-the-box provisioning connector with the solution	10	Select	0	
68	Solution must provide custom connector development framework.	10	Select	0	
69	Solution must provide manual provisioning capability (i.e. administrator-driven)?	10	Select	0	
70	Solution must support retry if a transaction fails	10	Select	0	
71	Solution must provide a toolkit for creating connectors for custom or homegrown applications	10	Select	0	
K	Identity Analytics				
72	Solution must support analytics capabilities to access the risk associated to the user and its access.	10	Select	0	
73	Solution must provide recommendation for remediation action based on user's access like suspend/disable account or trigger access review request for user.	10	Select	0	
74	Solution must provide comprehensive analytical reporting capabilities to assist with the cleansing of risky or excessive access	10	Select	0	
75	Solution must provide a report which outlines defined security risks by application	10	Select	0	
76	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	Select	0	
77	Solution must have capability for assignment of unique risk values to each application, entitlement and role within the system	10	Select	0	
78	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	Select	0	
79	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	Select	0	
80	Solution must provide dashboard with various insights like risky user, risky application, risky access, critical violation.	10	Select	0	
81	Solution must notify responsible parties / application owner when policy violations are detected.	10	Select	0	
82	Solution must be 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	Select	0	
L	Role Mining				
83	Solution must support both technical roles (Bottom-up) and business roles (top down) Role Modeling in GUI with graphical hierarchy support.	10	Select	0	
84	Solution must support linking Business-to-Technical Role Mapping or entitlements with nested role views with context and complete provisioning capabilities	10	Select	0	
85	Solution must have built-in Service on Demand enforcement so that it is embedded with policies, real-time conflict checks during role assignment.	10	Select	0	
86	Solution must support advanced mining using access analyzer with usage clustering providing richer pattern detection from user behavior	10	Select	0	
M	Single Sign-On (SSO)				
87	Single sign on portal should get deployed fully on premise	10	Select	0	
88	SSO portal must support multiple login mechanisms				
88.1	Two factor authentication	10	Select	0	
88.2	Email authentication	10	Select	0	
88.3	SMS authentication	10	Select	0	
88.4	chain authentication (combining with AD password)	10	Select	0	
88.5	one time link authentication	10	Select	0	
89	SSO solution should have the capabilities to integrate with different applications using SAML protocol	10	Select	0	
90	SSO solution should have the capability to include OIDC protocol if needed.	10	Select	0	
91	The SSO solution can be installed in any OS provided (Linux or Windows)	10	Select	0	
92	The administration of the solution must be protected by 2FA	10	Select	0	
93	The SSO solution should have the capability to send audit logs to external syslog server	10	Select	0	
94	The SSO solution must send verification emails to the users with any changes to his profile	10	Select	0	
95	Enables users to log in everywhere with a single identity, and for administrators to manage access based on that identity	10	Select	0	
96	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	Select	0	
Total		1030		0	

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

MFA

Multi-factor authentication (MFA)					
S. No.	Technical Specifications	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	The MFA solution must be support -> On-demand authenticator (Short Message System) -> Software authenticator -> Hardware Authenticators	10	Select	0	
2	The proposed solution should be deployed completely on-premises without any dependency on cloud	10	Select	0	
3	The MFA authentication server must be available in hardware appliance or software form purpose built for 2FA Application by the OEM.	10	Select	0	
4	The MFA server must come with a RADIUS server with no additional cost.	10	Select	0	
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	Select	0	
6	Solutions should be capable for integration with TACACS solution being used by the Bank.	10	Select	0	
7	The MFA server must support IETF RFC4758 (Cryptographic Token Key Initiation Protocol) protocol out-of-the-box with no additional customization required.	10	Select	0	
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	Select	0	
8.2	• Latest Microsoft Active Directory	10	Select	0	
9	The MFA server must support multiple replicas when necessary without any additional cost and licenses	10	Select	0	
10	The MFA solution should support FIDO2-compliant MFA tokens	10	Select	0	
11	The authentication agents must support the following platforms:				
11.1	Microsoft Windows 64 Bit Platforms Windows Server	10	Select	0	
11.2	Apache Web Server	10	Select	0	
11.3	Red Hat Enterprise Linux	10	Select	0	
11.4	IBM AIX	10	Select	0	
11.5	Solaris	10	Select	0	
11.6	SUSE Linux	10	Select	0	
11.7	Oracle Linux	10	Select	0	
11.8	Epic Hyperdrive	10	Select	0	
11.9	Rocky Linux	10	Select	0	
11.10	CentOS	10	Select	0	
12	MFA solution must support on-premises deployment.	10	Select	0	
13	The MFA server must be able to support software authenticators for the following platforms: 1. Smartphones a. Android devices b. iOS devices c. Laptops and Desktops d. Microsoft Windows & MAC OS	10	Select	0	
14	Solution should support adaptive authentication	10	Select	0	
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	Select	0	
A	Self Service Module				
16	Self Service portal must include the following functions:				
16.1	Authenticator Enrollment	10	Select	0	
16.2	Request token	10	Select	0	
16.3	Replace token	10	Select	0	
16.4	Change/Set PIN	10	Select	0	
16.5	Resync token	10	Select	0	
16.6	Clear Security Questions	10	Select	0	
16.7	Test Authenticator	10	Select	0	
16.8	Report Lost Authenticator & Active Directory Password change and reset.	10	Select	0	

MFA

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	Select	0	
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	Select	0	
Total		350		0	

Sr. No.	Category	Privileged Identity Management (PIM)/Privileged Access Management (PAM)	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Solution Overview	The proposed solution shall provide an integrated Privileged Identity Management (PIM)/Privileged Access Management (PAM) platform for centralized governance, control, monitoring, and protection of privileged identities and accounts.	10	Select	0	
2	Enterprise Deployment	The solution shall support deployment in on-premises, private cloud, public cloud, hybrid cloud, and virtualized environments.	10	Select	0	
3	Architecture	The architecture shall be modular, scalable, and support distributed deployment across DC and DR sites.	10	Select	0	
4	Disaster Recovery	The solution shall support synchronized disaster recovery deployment with configurable RPO and RTO.	10	Select	0	
5	Scalability	The solution shall support horizontal and vertical scalability without service interruption.	10	Select	0	
6	Centralized Management	The solution shall provide a centralized management console for administration, configuration, policy management, monitoring, and reporting.	10	Select	0	
7	Multi-Tenancy	The solution shall support logical segregation of multiple business units or subsidiaries.	10	Select	0	
8	Role Based Administration	The solution shall support granular RBAC with configurable administrative roles and segregation of duties.	10	Select	0	
9	Authentication	The solution shall integrate with enterprise identity providers including Active Directory, LDAP, SAML 2.0, OAuth 2.0, and OpenID Connect.	10	Select	0	
10	MFA	The solution shall support native multi-factor authentication and/or integration with MFA solutions.	10	Select	0	
11	Privileged Account Discovery	The solution shall automatically discover privileged accounts across supported infrastructure.	10	Select	0	
12	Asset Discovery	The solution shall automatically discover managed assets including servers, databases, network devices, cloud resources, and applications.	10	Select	0	
13	Inventory Management	The solution shall maintain a centralized inventory of privileged identities, accounts, and managed systems.	10	Select	0	
14	Identity Classification	The solution shall classify privileged identities into human, machine, service, application, and emergency accounts.	10	Select	0	
15	Service Account Management	The solution shall discover, manage, rotate, and govern service account credentials.	10	Select	0	
16	Application Credential Management	The solution shall securely manage application credentials without exposing passwords.	10	Select	0	
17	Machine Identity Management	The solution shall support lifecycle management of machine identities and non-human identities.	10	Select	0	
18	Secret Management	The solution shall securely store and manage passwords, API keys, SSH keys, certificates, tokens, and application secrets.	10	Select	0	
19	Enterprise Vault	The solution shall provide a secure encrypted credential repository (vault or equivalent secure storage mechanism)	10	Select	0	
20	Encryption	Sensitive information shall be encrypted at rest and in transit using industry-standard cryptographic algorithms.	10	Select	0	
21	Password Policy	The solution shall support configurable password complexity, history, expiry, and reuse policies.	10	Select	0	
22	Password Rotation	The solution shall automatically rotate privileged passwords based on configurable schedules or events.	10	Select	0	
23	Password Reconciliation	The solution shall verify and synchronize credential changes across managed systems.	10	Select	0	
24	SSH Key Management	The solution shall discover, rotate, revoke, and audit SSH keys.	10	Select	0	
25	Certificate Management	The solution shall support management of privileged certificates and cryptographic identities.	10	Select	0	
26	API Key Management	The solution shall securely manage API keys and service tokens.	10	Select	0	
27	Credential Checkout	The solution shall provide controlled checkout and check-in of privileged credentials.	10	Select	0	
28	Password Disclosure	Password visibility shall be controlled through configurable approval workflows and masking.	10	Select	0	
29	Emergency Accounts	The solution shall manage emergency (break-glass) accounts with enhanced monitoring and audit controls.	10	Select	0	
30	Privileged Session Management	Support secure privileged session establishment and management without exposing credentials to end users.	10	Select	0	
31	Session Recording	The solution shall record privileged sessions for audit and forensic purposes.	10	Select	0	
32	Session Playback	Recorded sessions shall support indexed playback and search capabilities.	10	Select	0	
33	Session Monitoring	Security administrators shall be able to monitor active privileged sessions in real time.	10	Select	0	
34	Session Termination	Authorized administrators shall be able to terminate active sessions when required.	10	Select	0	
35	Command Monitoring	The solution shall capture commands executed during privileged sessions.	10	Select	0	
36	Command Control	The solution shall support allow/deny policies for privileged commands.	10	Select	0	

37	File Transfer Control	The solution shall monitor and control file transfers performed during privileged sessions.	10	Select	0	
38	Clipboard Control	The solution shall support policy-based control of clipboard operations during privileged sessions.	10	Select	0	
39	Remote Access	The solution shall provide secure privileged remote access without requiring VPN wherever applicable.	10	Select	0	
40	Jump Server Capability	Provide secure session proxy, jump-host, gateway, or equivalent secure privileged access mechanism.	10	Select	0	
41	Just-in-Time Access	The solution shall support temporary privileged access based on approved requests.	10	Select	0	
42	Just Enough Administration	The solution shall provide granular privilege assignment limited to authorized administrative tasks.	10	Select	0	
43	Access Approval	The solution shall support configurable approval workflows for privileged access requests.	10	Select	0	
44	Multi-Level Approval	The solution shall support hierarchical and multi-stage approval workflows.	10	Select	0	
45	Access Expiry	Privileged access shall automatically expire after the approved duration.	10	Select	0	
46	Access Revocation	The solution shall immediately revoke privileged access upon policy violation or administrative action.	10	Select	0	
47	Least Privilege	The solution shall enforce least privilege principles across all privileged identities.	10	Select	0	
48	Segregation of Duties	The solution shall support segregation of duties to prevent conflicting privileged assignments.	10	Select	0	
49	Audit Logging	The solution shall maintain immutable audit logs covering authentication, authorization, approvals, credential usage, privileged sessions, administrative activities, and policy changes.	10	Select	0	
50	Audit Trail	The solution shall maintain tamper-evident and searchable audit trails for all privileged activities.	10	Select	0	
51	Log Integrity	The solution shall protect audit logs from unauthorized modification or deletion.	10	Select	0	
52	Log Forwarding	The solution shall forward audit logs to enterprise SIEM platforms using industry-standard protocols.	10	Select	0	
53	Syslog Support	The solution shall support Syslog, CEF, JSON, REST APIs or equivalent mechanisms for event forwarding.	10	Select	0	
54	Real-time Alerts	The solution shall generate real-time alerts for suspicious privileged activities and policy violations.	10	Select	0	
55	Dashboard	The solution shall provide customizable dashboards for SOC analysts, administrators, auditors, and management.	10	Select	0	
56	Executive Reporting	The solution shall provide executive-level reports summarizing privileged access risks and compliance status.	10	Select	0	
57	Operational Reporting	The solution shall provide operational reports on password rotation, account discovery, session activity, and access requests.	10	Select	0	
58	Compliance Reports	The solution shall generate compliance reports aligned with regulatory and audit requirements.	10	Select	0	
59	Custom Reports	The solution shall support creation of user-defined reports and scheduled report generation.	10	Select	0	
60	Search Capability	The solution shall support full-text search across privileged accounts, sessions, audit logs, and activities.	10	Select	0	
61	Advanced Filtering	The solution shall support filtering based on user, asset, application, account type, location, and time.	10	Select	0	
62	Behaviour Analytics	Detect anomalous privileged behaviour using analytics, behavioural analysis, machine learning or equivalent techniques.	10	Select	0	
63	Risk Scoring	The solution should assign configurable risk scores to privileged identities and sessions.	10	Select	0	
64	Adaptive Access	The solution should support contextual or risk-based access decisions based on user, device, location, and time.	10	Select	0	
65	SIEM Integration	The solution shall integrate with industry-standard SIEM platforms using standard APIs or connectors.	10	Select	0	
66	SOAR Integration	The solution shall support integration with SOAR platforms for automated response workflows.	10	Select	0	
67	UEBA Integration	The solution should integrate with User and Entity Behaviour Analytics (UEBA) platforms.	10	Select	0	
68	ITSM Integration	The solution shall integrate with ITSM platforms for request, approval, incident, and change management workflows.	10	Select	0	
69	REST API	The solution shall expose secure REST APIs for administration, automation, and integration.	10	Select	0	
70	SDK Support	The solution should provide SDKs or documented APIs for automation and integration.	10	Select	0	
71	Scripting	The solution shall support automation using scripting or API-based orchestration.	10	Select	0	
72	Directory Integration	The solution shall synchronize users and groups from enterprise directory services.	10	Select	0	
73	HRMS Integration	The solution should support integration with HRMS or authoritative identity sources for user lifecycle management.	10	Select	0	
74	Windows Support	The solution shall support Windows Server operating systems.	10	Select	0	

75	Linux Support	The solution shall support Linux operating systems.	10	Select	0	
76	Unix Support	The solution shall support Unix operating systems where applicable.	10	Select	0	
77	Network Devices	The solution shall support routers, switches, firewalls, load balancers, wireless controllers, and other network devices.	10	Select	0	
78	Security Appliances	The solution shall support privileged management of security appliances and security management platforms.	10	Select	0	
79	Hypervisors	The solution shall support major virtualization platforms through supported connectors or APIs.	10	Select	0	
80	Public Cloud	The solution shall support privileged identity governance for major public cloud providers.	10	Select	0	
81	Private Cloud	The solution shall support private cloud environments and cloud management platforms.	10	Select	0	
82	SaaS Applications	The solution shall support governance of privileged access to SaaS applications.	10	Select	0	
83	Containers	The solution should support privileged access for container platforms.	10	Select	0	
84	Kubernetes	The solution should support privileged administration of Kubernetes clusters.	10	Select	0	
85	DevOps Integration	The solution should support secure integration with DevOps pipelines and automation platforms.	10	Select	0	
86	CI/CD Integration	The solution should integrate with CI/CD tools using secure credential management.	10	Select	0	
87	Secret Injection	The solution should support secure runtime retrieval of secrets by applications and automation tools.	10	Select	0	
88	API Credential Governance	The solution shall manage lifecycle and protection of API credentials.	10	Select	0	
89	Certificate Lifecycle	The solution should support lifecycle management of digital certificates used for privileged access.	10	Select	0	
90	Key Management	The solution should support secure management of cryptographic keys or integration with enterprise key management systems.	10	Select	0	
91	HSM Integration	The solution should support integration with industry-standard Hardware Security Modules where required.	10	Select	0	
92	Backup	The solution shall support secure backup of configurations, vault contents, policies, and audit information.	10	Select	0	
93	Restore	The solution shall support restoration of backed-up data with integrity validation.	10	Select	0	
94	Health Monitoring	The solution shall continuously monitor component health, availability, and operational status.	10	Select	0	
95	Database Support	The solution shall support enterprise-grade relational database platforms or embedded databases as per OEM architecture.	10	Select	0	
96	Database Encryption	All repository data shall be encrypted at rest using industry-standard cryptographic algorithms.	10	Select	0	
97	Data Integrity	The solution shall validate integrity of configuration, vault, and audit data to prevent unauthorized modification.	10	Select	0	
98	Version Control	The solution shall maintain version history of policies, workflows, and administrative configurations.	10	Select	0	
99	Policy Management	The solution shall provide centralized creation, approval, deployment, rollback, and lifecycle management of security policies.	10	Select	0	
100	Change Tracking	The solution shall record all configuration changes with user, timestamp, previous value, and new value.	10	Select	0	
101	Policy Simulation	The solution should support validation or simulation of policy changes prior to deployment where technically feasible.	10	Select	0	
102	Bulk Administration	The solution shall support bulk onboarding, bulk updates, and bulk administrative operations.	10	Select	0	
103	Delegated Administration	The solution shall support delegated administration with granular privileges.	10	Select	0	
104	Notification	The solution shall provide configurable notifications through email, SMS, webhook, or equivalent enterprise notification mechanisms.	10	Select	0	
105	Workflow Engine	The solution shall provide configurable workflow automation for privileged access requests and approvals.	10	Select	0	
106	Session Timeout	The solution shall automatically terminate inactive privileged sessions based on configurable timeout policies.	10	Select	0	
107	Concurrent Session Control	The solution shall support configurable limits on concurrent privileged sessions.	10	Select	0	
108	Passwordless Access	The solution should support passwordless privileged access using federated identity and secure session brokering where applicable.	10	Select	0	
109	Secure Remote Access	The solution shall provide secure privileged remote access without exposing privileged credentials to end users.	10	Select	0	
110	Third-Party Access	The solution shall provide controlled privileged access for vendors, contractors, auditors, and third-party users with full monitoring and audit trails.	10	Select	0	
111	Vendor Access Governance	The solution shall support time-bound, approval-based privileged access for external users.	10	Select	0	

112	Compliance Frameworks	The solution shall support compliance with applicable RBI Cyber Security Framework, ReBIT guidance, CERT-In Directions, ISO/IEC 27001, and other applicable regulatory requirements.	10	Select	0	
113	Audit Support	The solution shall provide reports and evidence required for internal, statutory, and regulatory audits.	10	Select	0	
114	Evidence Export	The solution shall support secure export of audit logs, reports, and session recordings for investigation purposes.	10	Select	0	
115	Data Retention	The solution shall support configurable retention policies for audit logs, recordings, and operational data in accordance with organizational requirements.	10	Select	0	
116	Archival	The solution shall support archival of historical audit and session data with secure retrieval capability.	10	Select	0	
117	Data Purging	The solution shall support policy-based archival and deletion of historical data after the configured retention period.	10	Select	0	
118	Secure Communications	All communications between solution components shall be protected using secure industry-standard protocols.	10	Select	0	
119	Cryptographic Agility	The solution should support migration to updated cryptographic algorithms through software updates or configuration without major redesign.	10	Select	0	
120	Secure APIs	Administrative APIs shall support authentication, authorization, encryption, and audit logging.	10	Select	0	
121	Security Hardening	The solution shall provide secure configuration guidelines and support hardening of all solution components.	10	Select	0	
122	Vulnerability Management	The OEM shall provide security patches, vulnerability advisories, and remediation guidance throughout the contract period.	10	Select	0	
123	Software Updates	The solution shall support controlled upgrades with rollback capability and minimal operational disruption.	10	Select	0	
124	Licensing	Licensing shall support future scalability without requiring replacement of deployed architecture.	10	Select	0	
125	Capacity Expansion	The solution shall support expansion of managed assets, privileged accounts, and concurrent sessions through modular licensing or equivalent mechanisms.	10	Select	0	
126	OEM Technical Support	The OEM shall provide 24×7×365 technical support with defined escalation procedures.	10	Select	0	
127	Documentation	Comprehensive installation, administration, operational, API, troubleshooting, and security documentation shall be provided.	10	Select	0	
128	Future Readiness	The solution architecture shall support future expansion for hybrid cloud, Zero Trust, identity governance, and emerging enterprise technologies.	10	Select	0	
129	Standards Compliance	The solution shall use open standards and documented interfaces to facilitate interoperability with enterprise systems.	10	Select	0	
130	Interoperability	The solution shall support integration with heterogeneous enterprise environments using standard protocols and APIs without requiring proprietary dependencies.	10	Select	0	
131	Identity Correlation	The solution shall correlate privileged identities across multiple identity repositories to eliminate duplicate or orphaned privileged accounts.	10	Select	0	
132	Orphan Account Detection	The solution shall identify orphaned, inactive, dormant, and shared privileged accounts and generate periodic reports.	10	Select	0	
133	Shared Account Governance	The solution shall govern shared privileged accounts through individual accountability, approvals, and session attribution.	10	Select	0	
134	Credential Ownership	The solution shall maintain ownership information for every privileged credential and identity.	10	Select	0	
135	Periodic Recertification	The solution shall support configurable periodic recertification of privileged identities, entitlements, and access approvals.	10	Select	0	
136	Access Review	The solution shall support manager-, application owner-, and security owner-based privileged access reviews.	10	Select	0	
137	Dormant Credential Detection	The solution shall identify privileged credentials that have not been used for configurable periods.	10	Select	0	
138	Privileged Risk Dashboard	The solution shall provide dashboards indicating privileged account exposure, unused privileges, stale credentials, and policy violations.	10	Select	0	
139	Session Watermarking	The solution should support configurable session watermarking for privileged sessions.	10	Select	0	
140	Live Session Intervention	Authorized administrators shall be able to suspend, terminate, or quarantine suspicious privileged sessions.	10	Select	0	
141	Dual Control	The solution shall support dual authorization for sensitive administrative functions, wherever required.	10	Select	0	
142	Four-Eyes Principle	The solution should support two-person approval for predefined high-risk privileged operations.	10	Select	0	
143	Dynamic Access Policies	Access decisions shall support contextual conditions including time, device, location, business justification, and asset criticality.	10	Select	0	

144	Risk-Based Policies	The solution should allow dynamic modification of access privileges based on configurable risk scores.	10	Select	0	
145	Device Trust	The solution should evaluate endpoint posture through integration with enterprise security controls where available.	10	Select	0	
146	Time-Based Access	Privileged access shall be restricted to approved maintenance windows or business schedules where configured.	10	Select	0	
147	Geo-Restriction	The solution shall support configurable geographic restrictions for privileged authentication where applicable.	10	Select	0	
148	Concurrent Login Detection	The solution shall detect and report simultaneous privileged logins from multiple locations.	10	Select	0	
149	Privileged Session Isolation	Privileged sessions shall be logically isolated from end-user systems to minimize credential exposure.	10	Select	0	
150	Browser Isolation	The solution should support browser-based privileged access without exposing privileged credentials to endpoints.	10	Select	0	
151	Session Metadata	The solution shall capture user, source, destination, protocol, commands, timestamps, and duration for each privileged session.	10	Select	0	
152	Session Search	The solution shall support indexed searching of recorded sessions using metadata and commands executed.	10	Select	0	
153	Session Retention	The solution shall support configurable retention of privileged session recordings based on organizational policy.	10	Select	0	
154	Secure Recording Storage	Session recordings shall be protected against tampering and unauthorized access.	10	Select	0	
155	API Security	Administrative APIs shall support role-based authorization, authentication, rate limiting, and audit logging.	10	Select	0	
156	Open Standards	The solution shall use documented and standards-based interfaces to facilitate interoperability.	10	Select	0	
157	Connector Framework	The solution shall provide native or extensible connectors for enterprise applications and infrastructure.	10	Select	0	
158	Legacy Platform Support	The solution should support integration with legacy operating systems and business applications through supported mechanisms.	10	Select	0	
159	Cloud Identity Governance	The solution shall support privileged identity governance for cloud-native administrative identities.	10	Select	0	
160	Hybrid Identity	The solution shall provide a unified governance model for on-premises and cloud privileged identities.	10	Select	0	
161	SaaS Administration	The solution shall support governance of privileged administrative access to SaaS applications.	10	Select	0	
162	Kubernetes Administration	The solution should support privileged access management for Kubernetes administrative identities.	10	Select	0	
163	Container Secrets	The solution should support secure management of secrets used by containerized workloads.	10	Select	0	
164	DevOps Integration	The solution should support secure integration with DevOps and Infrastructure-as-Code workflows using APIs and secure secret retrieval.	10	Select	0	
165	Service Principal Governance	The solution shall support lifecycle management of service principals and equivalent non-human identities.	10	Select	0	
166	Secret Rotation APIs	The solution shall expose APIs to automate secret rotation for enterprise applications.	10	Select	0	
167	Credential Checkout Audit	Every credential checkout and check-in shall be fully audited.	10	Select	0	
168	Password Exposure Control	Password disclosure shall be restricted through configurable policies and approval workflows.	10	Select	0	
169	Compliance Evidence	The solution shall generate evidence required for internal, external, and regulatory audits.	10	Select	0	
170	Regulatory Mapping	Reports shall support mapping to applicable regulatory and organizational control frameworks.	10	Select	0	
171	Administrative Segregation	The solution shall support separation of infrastructure administration, security administration, and audit functions.	10	Select	0	
172	Immutable Audit Repository	Audit information shall be protected against unauthorized alteration using appropriate integrity controls.	10	Select	0	
173	Secure Upgrade	The solution shall support software upgrades while preserving configurations, policies, and audit information.	10	Select	0	
174	Configuration Validation	The solution shall validate configuration consistency following upgrades or restoration.	10	Select	0	
175	Administrative Audit	All administrative configuration changes shall be logged with before-and-after values where applicable.	10	Select	0	
176	Data Export	The solution shall support export of reports and audit records in standard formats.	10	Select	0	
177	Data Import	The solution shall support secure import of users, assets, policies, and configuration information.	10	Select	0	
178	Notification Templates	The solution shall support configurable notification templates for approvals, alerts, and operational events.	10	Select	0	

179	Time Synchronization	All solution components shall support synchronization with enterprise time sources to ensure consistent audit timestamps.	10	Select	0	
180	Policy Compliance Dashboard	The solution shall display compliance status of configured security policies across managed assets.	10	Select	0	
181	Emergency Override Logging	All emergency privileged access activities shall be separately identified and reported.	10	Select	0	
182	Administrative Lockout	The solution shall support configurable controls to protect against repeated failed administrative authentication attempts.	10	Select	0	
183	Secure Communication	Communication between solution components shall use authenticated and encrypted channels.	10	Select	0	
184	Machine Identity Security	Govern certificates, workload identities, service principals, Kubernetes identities, and API identities throughout their lifecycle.	10	Select	0	
185	Enterprise Secrets Management	Discover, rotate, audit, and manage secrets used by applications, DevOps, databases, and cloud workloads—not just administrator passwords.	10	Select	0	
186	Cloud PAM	The proposed solution should support Natively or through OEM-supported modules, licensed components the governance for AWS, Azure, GCP, OCI, Kubernetes, OpenShift, Microsoft 365, and SaaS administrative identities.	10	Select	0	
187	Zero Trust PAM	Continuous verification, adaptive authentication, contextual authorization, JIT access, device posture evaluation, and session risk scoring.	10	Select	0	
188	Third-Party Vendor Access	Dedicated workflows for vendors, OEM engineers, auditors, and contractors with time-bound access and monitoring.	10	Select	0	
189	Identity Threat Detection & Response (ITDR)	Detect anomalous privileged behaviour, privilege escalation, credential abuse, and identity attacks, with integration into SOC/SIEM.	10	Select	0	
190	Passwordless Administration	Support passwordless privileged authentication using enterprise identity providers where applicable.	10	Select	0	
191	General	The solution shall automatically discover machine identities, including service principals, workload identities, certificates, API identities, and non-human accounts across enterprise infrastructure.	10	Select	0	
192	General	The solution shall maintain a centralized inventory of machine identities with ownership, associated assets, lifecycle status, expiry, and risk classification.	10	Select	0	
193	General	The solution shall support lifecycle management of machine identities, including provisioning, onboarding, rotation, renewal, suspension, revocation, and decommissioning, as applicable.	10	Select	0	
194	General	The solution shall detect orphaned, dormant, expired, duplicate, or unused machine identities and generate reports.	10	Select	0	
195	General	The solution shall support automated or policy-driven rotation of credentials associated with machine identities, where technically supported.	10	Select	0	
196	General	The solution shall generate alerts for unauthorized usage of privileged machine identities.	10	Select	0	
197	General	The solution shall support lifecycle management of machine identities, including provisioning, rotation, renewal, suspension, and decommissioning.	10	Select	0	
198	General	The solution shall support automated rotation of credentials associated with machine identities.	10	Select	0	
199	General	The solution shall provide centralized management of enterprise secrets, including passwords, API keys, SSH keys, tokens, certificates, encryption keys, application credentials, and equivalent secret types.	10	Select	0	
200	General	The solution shall automatically discover secrets stored within enterprise infrastructure where technically supported.	10	Select	0	
201	General	The solution shall support automated or policy-driven rotation of privileged secrets based on configurable organizational policies.	10	Select	0	
202	General	The solution shall support secure runtime retrieval of secrets by applications through APIs or equivalent mechanisms.	10	Select	0	
203	General	The solution shall provide audit trails for all secret access, rotation, and retrieval operations.	10	Select	0	
204	General	The solution shall support secure archival and deletion of retired secrets.	10	Select	0	
205	General	The solution shall implement least-privilege principles for all privileged identities.	10	Select	0	
206	General	The solution shall support time-bound privileged access provisioning through Just-in-Time (JIT) access or equivalent temporary privileged access mechanisms.	10	Select	0	
207	General	The solution shall support granular privilege assignment implementing Just-Enough Administration (JEA) principles or equivalent least-privilege administrative controls.	10	Select	0	
208	General	The solution shall support contextual access policies based on user, device, location, application, business justification, and time.	10	Select	0	
209	General	The solution shall support adaptive and/or risk-based authentication using configurable enterprise security policies.	10	Select	0	
210	General	The solution shall continuously evaluate privileged sessions using analytics, behavioural analysis, machine learning, or equivalent mechanisms and generate alerts for anomalous activities.	10	Select	0	

211	General	The solution shall support privileged identity governance for public, private, and hybrid cloud environments.	10	Select	0	
212	General	The solution shall discover cloud administrative identities, privileged roles, and equivalent administrative entities across supported cloud platforms.	10	Select	0	
213	General	The solution shall govern privileged access for cloud-native services and management consoles.	10	Select	0	
214	General	The solution shall support management of cloud service accounts and non-human identities.	10	Select	0	
215	General	The solution shall provide reporting of cloud privileged access activities.	10	Select	0	
216	General	The solution shall support cloud policy enforcement through native capabilities, OEM-supported integrated components, or standards-based integration mechanisms.	10	Select	0	
217	General	The solution shall support secure privileged access for vendors, OEM engineers, contractors, consultants, auditors, and other external users.	10	Select	0	
218	General	The solution shall support sponsor-based, approval-based, or policy-driven onboarding of third-party privileged users.	10	Select	0	
219	General	The solution shall provide configurable approval workflows before granting third-party privileged access.	10	Select	0	
220	General	The solution shall automatically revoke third-party access upon completion of the approved access period.	10	Select	0	
221	General	The solution shall record and monitor all third-party privileged sessions.	10	Select	0	
222	General	The solution shall generate dedicated reports covering third-party privileged activities.	10	Select	0	
223	General	The solution shall support periodic recertification of privileged accounts and entitlements.	10	Select	0	
224	General	The solution shall generate compliance reports aligned with organizational and regulatory requirements.	10	Select	0	
225	General	The solution shall maintain immutable or tamper-evident audit trails for privileged activities.	10	Select	0	
226	General	The solution shall support configurable retention of audit records in accordance with organizational policies.	10	Select	0	
227	General	The solution shall support export of audit evidence in industry-standard formats.	10	Select	0	
228	General	The solution shall provide secure APIs for integration with enterprise automation workflows.	10	Select	0	
229	General	The solution shall support secure retrieval of credentials by applications and automation tools.	10	Select	0	
230	General	The solution shall support automated credential rotation for DevOps, CI/CD, Infrastructure-as-Code, and automation environments, where applicable.	10	Select	0	
231	General	The solution shall support API-based lifecycle management of privileged credentials.	10	Select	0	
232	General	The solution shall maintain audit logs for automated privileged operations.	10	Select	0	
233	General	The solution shall provide health monitoring of all solution components.	10	Select	0	
234	General	The solution shall support capacity monitoring and trend analysis.	10	Select	0	
235	General	The solution shall support backup validation and restoration verification.	10	Select	0	
236	General	The solution shall provide configurable operational dashboards.	10	Select	0	
237	General	The solution shall support automated notifications using email, webhooks, APIs, messaging services, or equivalent enterprise notification mechanisms.	10	Select	0	
238	General	The solution shall support open standards and documented APIs to facilitate interoperability with existing and future enterprise systems.	10	Select	0	
239	General	The solution shall support modular expansion to accommodate additional managed assets, privileged identities, and concurrent sessions without architectural redesign.	10	Select	0	
240	General	The solution should provide extensibility to support emerging enterprise identity technologies through standards-based integration.	10	Select	0	
241	General	The proposed solution shall support compliance with applicable directions, advisories, and guidelines issued by RBI, ReBIT, CERT-In, MeitY, and other competent Government of India authorities, as applicable to the Bank.	10	Select	0	
242	General	The solution shall support timely implementation of security updates, configuration changes, and mitigation measures in response to newly disclosed vulnerabilities and cyber threats.	10	Select	0	
243	General	The solution shall provide mechanisms to identify managed privileged assets affected by published Common Vulnerabilities and Exposures (CVEs).	10	Select	0	
244	General	The solution shall support integration with enterprise Vulnerability Management solutions through documented APIs, connectors, or industry-standard interfaces.	10	Select	0	
245	General	The solution shall support risk-based prioritization of remediation activities based on asset criticality, privilege level, exploitability, and business impact.	10	Select	0	
246	General	The solution shall generate alerts for privileged systems impacted by critical or high-severity vulnerabilities.	10	Select	0	

PIM/PAM

247	General	The solution shall maintain audit records of remediation actions, emergency access approvals, and security policy changes undertaken in response to cyber threats.	10	Select	0	
248	General	The solution shall support integration with Security Operations Centre (SOC), SIEM, SOAR, Threat Intelligence Platforms (TIP), Incident Response, and equivalent enterprise security platforms through documented APIs, connectors, or industry-standard interfaces.	10	Select	0	
249	General	The solution shall support automated notification and workflow initiation for critical security advisories and remediation activities.	10	Select	0	
250	General	The solution shall provide reporting on privileged assets pending remediation, overdue remediation, and remediation trends.	10	Select	0	
251	General	The solution shall support rapid response to zero-day and actively exploited vulnerabilities through configurable compensating security controls, emergency policy enforcement, temporary access restrictions, or equivalent mitigation mechanisms.	10	Select	0	
252	General	The solution shall support emergency policy deployment with minimal operational disruption, where technically feasible.	10	Select	0	
253	General	The solution shall identify privileged identities and systems affected by newly disclosed critical vulnerabilities.	10	Select	0	
254	General	The solution shall provide enhanced monitoring and recording of privileged sessions during declared high-risk security events.	10	Select	0	
255	General	The solution shall generate alerts when privileged credentials are used on systems affected by critical vulnerabilities.	10	Select	0	
256	General	The solution shall support emergency suspension or restriction of privileged access to compromised assets based on configurable policies.	10	Select	0	
257	General	The solution shall support preservation and secure export of privileged session records and audit logs for forensic investigation and regulatory requirements.	10	Select	0	
258	General	The solution shall support post-incident reporting and evidence generation for investigation and regulatory purposes.	10	Select	0	
259	General	The solution must deliver secured, verifiable email communication authenticated in alignment with the Privileged Trust Sureness Protocol or an equivalent industry-standard cryptographic mechanism that provides message authenticity, integrity, and non-repudiation	10	Select	0	
260	General	The proposed solution shall support Zero Trust security principles by continuously evaluating the trust posture. The Solution should support quarantine enforcement/policy based response actions	10	Select	0	
Total			2600		0	

DAM

Sr.No.	Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
1	Creation of an inventory through auto discovery of all databases and database users, deployed across the bank.	10	Select	0	
2	The proposed DAM solution should be able to monitor databases in scope without dropping any log.	10	Select	0	
3	The solution shall support horizontal and/or vertical scalability without requiring architectural redesign.	10	Select	0	
4	The solution should have the capability to detect vulnerabilities including behavioral vulnerabilities such as excessive administrative logins, account sharing and unusual after-hours' activity by scanning databases, data warehouses and big data environments. The solution should identify issues such as missing patches, weak passwords, unauthorized changes and misconfigured privileges. Further, comprehensive reports should be provided along with suggestions to address all vulnerabilities.	10	Select	0	
5	The solution should provide capability to detect DB attacks and prevent attacks such as SQL injection, leakage of sensitive data etc. and should be able to detect and alert unauthorized or unusual queries, access to sensitive and confidential data etc. for various database including big database.	10	Select	0	
6	The solution should support installation manager on each database server to avoid manual efforts to coordinate agent activities along with up-gradation and configuration changes.	10	Select	0	
7	The solution should be able to monitor, detect and prevent breaches/anomalies for following databases: a) MySQL b) MS SQL c) PostgreSQL d) Oracle DB e) Maria DB f) any other DBs	10	Select	0	
8	The solution should identify, auto-classify the data/database objects based on confidentiality and sensitivity of data based on SPDI, PII, ISO 27001 or custom parameters.	10	Select	0	
9	The solution should audit all types of database access across the organization regardless of database type or operating system of the host without relying on native auditing.	10	Select	0	
10	The solution should be capable of performing real-time monitoring and recording of all database activities like DDL, DML and DCL, schema creation, modification of accounts/roles and privileges.	10	Select	0	
11	The solution should capture and analyse all database activities from both application user and privileged user accounts, providing detailed audit trails that show the "Who, What, When, Where, and How" of each transaction.	10	Select	0	
12	The solution should be able to inspect SQL statements going to the database and determine with high accuracy whether to allow, log, audit, substitute or block the SQL.	10	Select	0	
13	The solution shall integrate with database encryption technologies where applicable and continue to monitor database activities on encrypted databases	10	Select	0	
14	The solution should be able to manage & record database access by user, time, application context, date, etc., and should be capable of traffic filtering, categorization, IP field-based on custom parameters (i.e., person, user system, user ID etc.).	10	Select	0	
15	The solution shall have minimal impact on database performance. OEM shall provide benchmark results and deployment best practices demonstrating negligible performance impact under recommended sizing.	10	Select	0	
16	The solution shall be able to integrate with leading Next-Gen SOC solutions such as SIEM, S-BDL, SOAR etc. to generate meaningful correlated events. Also, it should be capable of sending all format logs to SIEM/S-BDL	10	Select	0	
17	The solution should be able to integrate with ticketing management solutions like Manage Engine etc. for recording and logging change requests.	10	Select	0	
18	The solution should be capable of generating reports on policy console including usage of agents, pushing upgrades, push updates, configurations updates, policy updates, startup/restart etc.	10	Select	0	
19	The solution should have the capability to build an inventory by discovery of all databases and database users. The discovery capability by itself should be near real-time and on-demand discovery.	10	Select	0	
20	The solution should have the ability to generate reports consisting of the details of all database-level IP addresses, database type, Agent versions, status, etc. (active/inactive) and timestamp.	10	Select	0	

DAM

21	The solution should detect sensitive data types as defined by the bank such as user ID, email address, etc., in database queries.	10	Select	0	
22	The solution should enable segregation of duty in terms of account management, security administration and database administration.	10	Select	0	
23	The solution should have various notification mechanisms like Mails, SNMP traps etc. for security monitoring and health monitoring and the notification mechanism must be real time. Specify the notification mechanisms the solution supports.	10	Select	0	
24	The solution should be capable of identifying the missing patches and report the same and should have capabilities of virtual patching or protecting through security policies of known vulnerabilities till the patch is installed.	10	Select	0	
25	The solution should leverage AI/ML/behavioural analytics/ statistical analysis to: a) Fine tune database user policies to raise alerts in case of any abnormality in their activities. b) Reduce false positives to minimum and raise only actionable and materialistic alerts.	10	Select	0	
26	The 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	Select	0	
27	The solution should provide optimum utilization of resources by using Load balancing between its devices, if it is using multiple boxes/gateways and ensure the HA as required in the RFP	10	Select	0	
28	The solution must have tamper-proof log storage capability.	10	Select	0	
29	The proposed solution required monitoring should be delivered while solution is enabled and in blocking mode.	10	Select	0	
30	The solution should support creation of policies/rules for enforcing access control and proper rights management on databases.	10	Select	0	
31	The solution must support reporting of deviations to the policies and access control.	10	Select	0	
32	Solution should continuously learn the user and application behavior in respect of accessing a database. Learning should be a continuous process and should not stop after a certain stage.	10	Select	0	
33	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	Select	0	
34	DAM solution should identify abnormal server and user behavior and provide early detection of possible attacks using outliers. For example: a) User accessing a table for the first time. or b) Exceptional volume of errors.	10	Select	0	
35	Solution must support filtering/hiding of the bind variables of all the SQL activities captured.	10	Select	0	
36	The solution should not store sensitive data in plain text in logs generated by the application (e.g. passwords).	10	Select	0	
37	Logs and audit-trail generated by the solution should not be editable by users/administrator and should be read-only.	10	Select	0	
38	The solution shall support periodic security content, signature, rule and threat intelligence updates provided by the OEM.	10	Select	0	
39	Communication from agent to management server must be encrypted.	10	Select	0	
40	Solution also be able to monitor database which runs on non-standard port.	10	Select	0	
41	Solution should be able to auto classify the database/database-objects based on sensitivity and confidentiality of data based on PII, SPDI, PCIDSS guidelines or customized parameters.	10	Select	0	
42	The solution should be capable of auto discovering sensitive/confidential data, like credit card Numbers, Aadhaar or any PII in the database and offers the ability for customization.	10	Select	0	
43	The solution should be able to auto discover privilege users in the database and should support user entitlement reviews on database accounts.	10	Select	0	
44	The solution should identify insecure default accounts and weak/default credentials through database security assessment capabilities.	10	Select	0	
45	Solution tracks the dormant accounts as per defined rule.	10	Select	0	
46	The solution should inspect both in-coming and out-going DB traffic, compare with the rules and generate alert.	10	Select	0	

DAM

47	Solution should detect attacks on network protocols, as well as application layer DB activity.	10	Select	0	
48	The solution should provide full details needed for analysis of audited events: date and time, raw SQL, parameters used, end username, source IP, source application, destination database instance, schema DB objects affected, command details, results generated, values affected etc. should be capable of capturing and reporting at a very granular level.	10	Select	0	
49	Solution should detect attacks attempting to exploit known vulnerabilities as well as common threat vectors and can be configured to issue an alert and/or "terminate the session in real time or policy-based blocking"	10	Select	0	
50	The solution should discover misconfigurations in the database and its platform and suggest remedial measures.	10	Select	0	
51	The solution should be capable of reporting missing patches and report the details of such patches and vulnerabilities associated with.	10	Select	0	
52	Solution should have capability to track execution of stored procedures, including who executed a procedure, what procedure name and when, which tables were accessed.	10	Select	0	
53	Solution should also be able to detect any change happens in stored procedure.	10	Select	0	
54	The 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	Select	0	
55	The proposed DAM solution shall identify, monitor, audit and report all access to sensitive data and sensitive database objects based on Bank-defined or regulatory classifications.	10	Select	0	
56	The solution support creation of different type of security and audit policies such as rule, report based on heuristic and content based. These policies should support customization.	10	Select	0	
57	Ability to kill sessions for accessing sensitive data/policy violations and keeping all activity in the logs.	10	Select	0	
58	The solution should be capable of blocking access real time, execution of commands which violate the rules/policies, store the events securely and report the same in real time.	10	Select	0	
59	The Proposed solution 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 malicious queries including blocking of matching signatures for known attacks like SQL injection.	10	Select	0	
60	The solution should support installation of agents, update of agents, configurations updates, policy updates, start/stop/restart etc. at all the databases from management server centrally.	10	Select	0	
61	The agent deployment/activation should not require a reboot of OS and DB services (except in case database is using native encryption feature) after installation/configuration. Only one OEM DAM agent to be installed, if required. All agents regardless of deployment mode should be managed from the centralized management console.	10	Select	0	
62	If the agent malfunctions or is uninstalled or disabled on server, immediate alert to be issued.	10	Select	0	
63	If the communication between agent and the console is lost, immediate alert to be issued.	10	Select	0	
64	The solution shall provide comprehensive auditing capabilities and should not rely solely on native database audit logs.	10	Select	0	
65	The solution should be able to support/monitor all database activities in OS like all flavors of Linux (Solaris, CentOS, Ubuntu, RHEL) and Windows for databases like MS SQL, MySQL, PostgreSQL, Oracle DB, Maria DB, any other DBs etc. at a minimum provided that DB vendors still support the versions in scope.	10	Select	0	
66	The solution should provide information of DB links and should have capability to monitor the activity of DB links.	10	Select	0	
67	The solution should generate alert for any violation of security policy in real time.	10	Select	0	
68	All reports should be generated on-demand or by scheduling.	10	Select	0	
69	The solution should discover all the databases with details i.e. IP, type, OS, available in the bank network.	10	Select	0	

DAM

70	The solution should also discover if any new database and DB objects created within the monitored network/systems.	10	Select	0	
71	The solution should log the actual client IP.	10	Select	0	
72	The solution should profile the activities to filter noise or known false positives and should generate alert if any violation.	10	Select	0	
73	Separate policies should be applied for different databases configured in DAM.	10	Select	0	
74	The solution should have pre-built templates for well-known security and audit policies.	10	Select	0	
75	The proposed solution shall support monitoring of all databases covered under the procured licenses and shall support future expansion. Solution should support the deployment modes i.e. monitoring / blocking separately for each database.	10	Select	0	
76	The solution shall provide mechanisms to optimize resource utilization and configurable resource consumption	10	Select	0	
77	The solution should have capability to facilitate rule creation at a very granular level. Example: Which user can connect from which source, access what objects, have which rights, at what time window etc.	10	Select	0	
78	Rules also should allow blocking access depending upon different parameters like above.	10	Select	0	
79	The Proposed Solution should include a Web based single administration interface.	10	Select	0	
80	The Proposed solution should be managed centrally for Both DCs setup.	10	Select	0	
81	Management solution should support Role-Based Access Control or multiple user roles that facilitate separation of duties, i.e. Administrator (Super-User), Manager, Read Only, etc.	10	Select	0	
82	The solution shall support inbuilt authentication and integration with enterprise Identity and Access Management (IAM) platforms, including LDAP/Active Directory, RADIUS, SAML, TACACS+, and other industry-standard authentication mechanisms.	10	Select	0	
83	The Bank should be able to deploy or remove the DAM solution from the network with no impact on the existing databases or the network architecture.	10	Select	0	
84	Support proper reporting and logging facilities.	10	Select	0	
85	Should be able to report events and alerts via standard mechanisms, for example, to a syslog or SNMP server or a SIEM solution.	10	Select	0	
86	The solution shall support configurable/custom log message formats with dynamic field substitution.	10	Select	0	
87	The solution must support generation of both predefined as well as custom-built reports as per Bank's requirements with both tabular views, PDF and data analysis graphical views.	10	Select	0	
88	The solution should have easy option to customize report without developing or requiring lot of customization/changes from scratch.	10	Select	0	
89	Alert should be generated in case of violation of rules through SMTP (mail).	10	Select	0	
90	The 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	Select	0	
91	The solution should be able to generate the reports in PDF, Excel & CSV formats.	10	Select	0	
92	Solution must support either: 1) Ability to query raw event data via REST API, 2) Ability to perform bulk exports of raw event data, or 3) Other external analytical and data store integration method.	10	Select	0	
93	The solution shall store audit logs in a secure, tamper-evident repository supporting integrity verification and efficient retrieval.	10	Select	0	
94	Solution should provide monitoring of all on-prem databases via centralized management console.	10	Select	0	
95	Permanent audit logs shall be securely transmitted and centrally stored in the DAM management platform	10	Select	0	
96	The solution should have a lean architecture with minimal moving parts	10	Select	0	
97	The solution should automate and simplify regulatory compliance activities and provides superior long-term retention of live audit data in the DAM. It should enable long-term data estate and forensic records retention policies (e.g., fast access, live audit data, length of retention timeframes).	10	Select	0	

DAM

98	The solution shall support databases deployed on on-premises, private cloud, public cloud, Database-as-a-Service (DBaaS) and virtualized environments.	10	Select	0	
99	The solution shall support configurable forwarding of events, alerts and logs to SIEM/SOAR platforms	10	Select	0	
100	The Solution must have in-built Risk Analytics module/engine.	10	Select	0	
101	The Risk Analytics module/engine must be purposefully built and be self-contained	10	Select	0	
102	The Risk Analytics module/engine should provide unified console which aggregates threat indicators across the enterprise databases.	10	Select	0	
103	The Risk Analytics module/engine should provide an intuitive dashboard page containing widgets that give a quick informative and drill-down capability view of the following: a) Protected Assets b) Open Issues c) Security Events Over Time d) Entities With Most Severe Incidents e) Events Analyzed f) System Health Status	10	Select	0	
104	The Risk Analytics Solution must be able to support the identification of anomalous activity on databases including: a) MS SQL b) MySQL c) PostgreSQL d) Oracle DB e) Maria DB f) any other DB deployed in Bank	10	Select	0	
105	The Risk Analytics Solution must provide behavior analytics algorithm to establish behavioral baseline and find deviations.	10	Select	0	
106	The Risk Analytics Solution must be able to differentiate between suspicious behavior from risky/abusive behavior (anomaly vs incident).	10	Select	0	
107	The Risk Analytics Solution should be able to assess user's risk potential.	10	Select	0	
108	The solution should support real-time monitoring and policy enforcement/blocking for Cloud DB/DBaaS environments, including databases deployed on Kubernetes/container platforms.	10	Select	0	
109	The solution should provide a Compliance Smart Assistant capable of automatically deploying industry-standard compliance policies (PCI DSS, SOX, GDPR, HIPAA, etc.) with minimal manual configuration.	10	Select	0	
110	The solution should automatically terminate, quarantine, or block suspicious database sessions based on configurable security policies.	10	Select	0	
111	The solution should identify database user privileges, review excessive permissions, and detect inactive/dormant privileged accounts.	10	Select	0	
112	The solution should provide Data Risk Analytics by correlating activities, vulnerabilities, identities, and sensitive data across all monitored databases.	10	Select	0	
113	The solution should expose its security capabilities through a standardized protocol-based interface (MCP) enabling AI agents and orchestration platforms to dynamically discover and invoke platform capabilities without custom integration.	10	Select	0	
114	The Risk Analytics Solution should automatically detect the following: a) Nature of accounts which connect to the database (Service Account, DBA User Account, etc.) b) Purpose of database tables (Business Critical Tables, System Tables, etc.) c) Data access habits (working hours, amount of data retrieved)	10	Select	0	

DAM

115	The Risk Analytics Solution must be able to detect Abnormal Behavior such as: a) Database Access at Non-Standard Time b) Database Service Account Abuse c) Excessive Database Record Access d) Excessive Failed Logins e) Excessive Failed Logins from Application Server f) Excessive Multiple Database Access g) Machine Takeover h) Suspicious sensitive system tables scan i) Suspicious Application data access j) Suspicious Database command execution k) Suspicious Dynamic SQL activity	10	Select	0	
116	The Risk Analytics Solution must be able to identify/detect the following: a) Typical end point information b) Typical database access patterns	10	Select	0	
117	The Risk Analytics Solution 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	Select	0	
118	The 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	Select	0	
119	The Risk Analytics Solution must be able to integrate with Active Directory (AD) to enhance forensics and provide line of sight into user identity.	10	Select	0	
120	The Risk Analytics Solution should be able to perform analysis when integrated with Active Directory.	10	Select	0	
121	The Risk Analytics module shall provide user-centric dashboards with drill-down capabilities for incidents, anomalies, user behaviour and endpoint activity.	10	Select	0	
122	The Risk Analytics Solution must support REST API to enable extraction of Security Events.	10	Select	0	
123	All communications invoking API must be done over SSL.	10	Select	0	
124	The Risk Analytics Solution should be able to whitelist behavior which is authorized or acknowledge behavior that cannot be remediated immediately.	10	Select	0	
125	The Risk Analytics Solution must be able to send logs to SIEM or other Risk Analytics Solution for seamless incident management.	10	Select	0	
126	The Risk Analytics Solution must give incidents details which include Username, Source, Destination, Related/Correlated Issues, Type, Time, Severity and Priority.	10	Select	0	
127	The Risk Analytics Solution should automatically assign a Priority Score (a more granular threat score, on a defined scale) to each incident for easier classification of important events.	10	Select	0	
128	The Risk Analytics Solution should include comprehensive incident details when investigating an incident. Details should include: a) Description b) Severity Influencing Reasons c) Client and Server Details d) Incident Details e) Typical Behavior	10	Select	0	
129	The Risk Analytics Solution must be able to export detected incidents and anomalies to an Excel file for offline review.	10	Select	0	
130	The Risk Analytics Solution must be able to send email notification on detecting an issue/incident.	10	Select	0	
131	The solution shall provide executive dashboards showing overall database security posture, compliance status, risk trends and outstanding security issues across the enterprise.	10	Select	0	
Total		1310		0	

SBOM, CBOM & AI-BOM					
S. No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A	Infrastructure, deployment and integrations				
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	Select	0	
2	The solution must assess the relevance and impact of identified vulnerabilities, correlate them with affected software packages	10	Select	0	
3	The solution must provide integration with enterprise ticketing tools (ITSM Manage Engine)	10	Select	0	
4	The solution must automatically close the vulnerabilities once the corresponding tickets are closed in the ticketing solution.	10	Select	0	
5	The solution must offer API for other parties to integrate and report vulnerabilities specific to a component or software application.	10	Select	0	
6	The solution must integrate with diverse vulnerability databases and advisories	10	Select	0	
7	The solution must support Single Sign-On (SSO) with the identity provider.	10	Select	0	
8	The solution must be able to integrate with AD to map the applications to application owners in the AD.	10	Select	0	
B	Functional and Technical Requirements				
1	The platform shall ingest SBOMs in SPDX 2.3 and SPDX 3.0 formats.	10	Select	0	
2	The platform shall ingest SBOMs in CycloneDX 1.5 and 1.6 formats (JSON and XML).	10	Select	0	
3	The platform shall support SBOM ingestion via UI upload, REST API, CLI, CI/CD plugin (GitHub Actions, GitLab, Jenkins, Azure DevOps).	10	Select	0	
4	The platform shall auto-generate SBOMs from container images (Docker / OCI), OS package lists, code repositories, and binary artifacts.	10	Select	0	
5	Generated SBOMs shall conform to the NTIA Minimum Elements and the CERT-In SBOM minimum data fields: supplier, component name, version, unique identifier (PURL/CPE), dependency relationship, hash, license, SBOM author, and timestamp.	10	Select	0	
6	The platform shall deduplicate components across multiple SBOM sources so a component appearing in N sources appears as one inventory row with N source attributions.	10	Select	0	
7	The platform shall capture and display the full dependency tree including direct and transitive dependencies.	10	Select	0	
8	The platform shall store SBOM version history of the same SBOM.	10	Select	0	
9	The platform shall validate ingested SBOMs against schema and report validation errors with line-level detail.	10	Select	0	
10	The platform shall support bulk SBOM import/export in native CycloneDX/SPDX without re-encoding loss.	10	Select	0	
11	The platform shall scan the source code and generate CBOM info	10	Select	0	
12	The platform shall accept CBOM uploads in CycloneDX 1.6 cryptographic extension format (JSON and XML) via UI and REST API.	10	Select	0	
13	Uploaded CBOMs shall be schema-validated with line-level error reporting and rejected on schema failure.	10	Select	0	
14	The platform shall display the cryptographic inventory captured in an uploaded CBOM — algorithms, protocols, libraries, certificates, keys, and configurations — as read-only records attached to the relevant CMDB asset(s).	10	Select	0	
15	The platform shall maintain upload history and version diff for CBOMs of the same asset.	10	Select	0	
16	The platform shall support bulk CBOM import/export in native CycloneDX format without re-encoding loss.	10	Select	0	
17	The platform shall provide a unified inventory where SBOM components and uploaded CBOM cryptographic assets are attached to the business services.	10	Select	0	
18	A single risk view per asset shall display software vulnerabilities and cryptographic risks in one ranked queue.	10	Select	0	
19	A single remediation ticket may carry both SBOM- and CBOM-driven items for the same asset.	10	Select	0	
20	The platform shall support unified export of the SBOM + CBOM bundle for an application or business service for sharing with auditors / CERT-In empanelled auditors.	10	Select	0	
21	The platform shall continuously re-correlate ingested SBOMs against NVD and vendor advisories.	10	Select	0	
22	The solution shall support configurable compliance policies and metadata mapping aligned with organizational and regulatory requirements (e.g., CERT-In), while supporting BOM generation and ingestion	10	Select	0	
23	The solution must offer a secure way of receiving CBOM & SBOM for third party vendor products through a vendor portal.	10	Select	0	
24	The solution must offer a secure way of exchanging CBOM & SBOM information by the bank with signing auditors or regulatory bodies or shall support export of BOM in an industry-standard format (e.g., CycloneDX) suitable for secure sharing with auditors and regulatory bodies..	10	Select	0	
25	The solution should recognize all packages via binary or dependency resolution via package managers.	10	Select	0	
26	Solution should be able to detect open-source packages and report related vulnerabilities, outdated versions, and license compliance risk.	10	Select	0	

SBOM, CBOM, AI BOM AND QBOM

27	Solution shall support out of box capabilities to execute scan against a public git repository e.g., Github	10	Select	0	
28	Solution should support integrations to CI servers e.g., Jenkins, Azure DevOps, gitlabs etc	10	Select	0	
29	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	Select	0	
30	The solution must offer an ability to track components for internal tools and third party tools.	10	Select	0	
31	The solution shall support configurable cryptographic metadata and policy mapping to meet organization-specific regulatory reporting requirements.	10	Select	0	
32	The solution must offer per product view into the known and discovered vulnerabilities.	10	Select	0	
33	The solution must be able to generate CBOM (Cryptography Bill of Materials) with following details:				
33.1	· Cryptographic Component/Module Name, e.g., OpenSSL, Bouncy Castle	10	Select	0	
33.2	· Library Name and Version, e.g., OpenSSL v1.1.1k	10	Select	0	
33.3	· Cryptographic Algorithm Used, e.g., AES, RSA, SHA-256	10	Select	0	
33.4	· Key Length, e.g., 2048-bit, 256-bit	10	Select	0	
33.5	· Protocol Name and Version, e.g., TLS 1.2, SSH 2.0	10	Select	0	
33.6	· Certificate Expiry Date, To track upcoming expirations	10	Select	0	
33.7	· Key Expiry Date / Rotation Schedule, If keys have a defined lifecycle	10	Select	0	
33.8	· shall associate assets with their intended usage context (e.g., encryption, signing, hashing, secure transport)	10	Select	0	
33.9	· FIPS/NIST Compliance Status, Whether the crypto module is validated	10	Select	0	
33.10	· shall associate assets with their deployment or usage location through native asset metadata or configurable tagging mechanisms	10	Select	0	
44	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. This includes: · Remote Discovery & Access · Comprehensive Inventory Collection	10	Select	0	
45	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	Select	0	
46	The solution must support BOM import/export in interoperable formats.	10	Select	0	
47	There must be a single view of vulnerabilities from scanners, VAPT, bug bounty, etc. mapped to SBOM	10	Select	0	
48	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	Select	0	
49	The solution must be able to map severity-based prioritization of vulnerabilities at the application level.	10	Select	0	
50	The solution must offer a risk level distribution by vulnerability classification	10	Select	0	
51	The solution must convey the data about licenses used by each component.	10	Select	0	
52	The solution must offer a risk level distribution by License classification (permissive, reciprocal and restricted)	10	Select	0	
53	The proposed solution shall automatically discover all cryptographic assets deployed across enterprise applications and infrastructure.	10	Select	0	
54	The solution shall maintain an inventory of cryptographic algorithms, keys, certificates, protocols and cryptographic libraries.	10	Select	0	
55	The solution shall identify cryptographic usage across applications, APIs, operating systems, databases and middleware.	10	Select	0	
56	The solution shall discover TLS, SSL, SSH, IPSec and VPN cryptographic implementations.	10	Select	0	
57	The solution shall identify weak, deprecated and vulnerable cryptographic algorithms.	10	Select	0	
58	The solution shall identify SHA-1, MD5, DES, RC4 and other deprecated cryptographic algorithms.	10	Select	0	
59	The solution shall identify RSA, ECC and post-quantum cryptographic implementations.	10	Select	0	
60	The solution shall identify applications using vulnerable cryptographic libraries.	10	Select	0	
61	The solution shall provide dashboards for cryptographic posture and compliance.	10	Select	0	
62	The proposed solution shall automatically discover all AI, Machine Learning and Generative AI assets deployed across the enterprise.	10	Select	0	
63	The solution shall maintain a centralized inventory of Large Language Models (LLMs), Small Language Models (SLMs), AI Agents, RAG systems and AI APIs.	10	Select	0	

SBOM, CBOM, AI BOM AND QBOM

64	The solution shall maintain model metadata including model name, version, provider, deployment type, framework and hosting location.	10	Select	0	
65	The solution shall identify AI frameworks such as TensorFlow, PyTorch, ONNX, Hugging Face and equivalent technologies.	10	Select	0	
66	The solution shall discover AI model dependencies, embeddings, vector databases, plugins and external AI services.	10	Select	0	
67	The solution shall maintain AI supply chain relationships between models, datasets, prompts, APIs and inference services.	10	Select	0	
68	The solution shall correlate AI assets with software components identified through SBOM.	10	Select	0	
69	The solution shall correlate AI assets with cryptographic assets identified through CBOM.	10	Select	0	
70	The solution shall identify vulnerabilities associated with AI frameworks, libraries and dependencies.	10	Select	0	
71	The solution shall support AI risk assessment based on model criticality, exposure and dependency analysis.	10	Select	0	
72	The solution shall provide AI asset lineage and dependency visualization.	10	Select	0	
73	The solution shall support AI governance reporting and regulatory compliance.	10	Select	0	
74	The solution shall support AI-BOM generation in machine-readable formats for enterprise exchange.	10	Select	0	
75	The solution shall provide APIs for integration with CI/CD, DevSecOps, GRC and vulnerability management platforms.	10	Select	0	
76	The solution shall maintain complete audit trails for AI-BOM creation, updates and consumption.	10	Select	0	
77	The solution shall continuously update the AI-BOM whenever AI models, datasets or dependencies change.	10	Select	0	
78	The proposed solution shall automatically discover cryptographic assets across applications, operating systems, databases, middleware and network infrastructure.	10	Select	0	
79	The proposed solution shall maintain a centralized Cryptographic Bill of Materials (CBOM) repository.	10	Select	0	
80	The proposed solution shall inventory cryptographic algorithms, protocols, libraries, certificates and cryptographic keys.	10	Select	0	
81	The proposed solution shall identify cryptographic libraries embedded within software applications.	10	Select	0	
82	The proposed solution shall discover TLS, SSL, SSH, IPSec and VPN cryptographic implementations.	10	Select	0	
83	The proposed solution shall maintain an inventory of asymmetric, symmetric and hashing algorithms used across enterprise applications.	10	Select	0	
84	The proposed solution shall identify deprecated or insecure algorithms including MD5, SHA-1, DES, RC4 and equivalent legacy cryptographic mechanisms.	10	Select	0	
85	The proposed solution shall identify software components dependent on vulnerable cryptographic libraries.	10	Select	0	
86	The proposed solution shall correlate cryptographic assets with software components identified in SBOM.	10	Select	0	
87	The proposed solution shall generate cryptographic risk scores based on algorithm strength, usage and exposure.	10	Select	0	
88	The proposed solution shall provide dashboards for enterprise cryptographic posture and compliance.	10	Select	0	
89	The proposed solution shall automatically discover all Artificial Intelligence (AI), Machine Learning (ML), Generative AI and Agentic AI assets deployed across the enterprise.	10	Select	0	
90	The proposed solution shall maintain a centralized AI Bill of Materials (AI-BOM) repository.	10	Select	0	
91	The proposed solution shall inventory Large Language Models (LLMs), Small Language Models (SLMs), AI Agents and Retrieval-Augmented Generation (RAG) applications.	10	Select	0	
92	The proposed solution shall maintain metadata including model name, version, provider, framework and deployment environment.	10	Select	0	
93	The proposed solution shall identify AI frameworks, SDKs and model dependencies used by enterprise applications.	10	Select	0	
94	The proposed solution shall discover vector databases, embeddings, plugins and AI APIs associated with deployed AI applications.	10	Select	0	
95	The proposed solution shall correlate AI assets with SBOM and CBOM inventories to provide end-to-end supply chain visibility.	10	Select	0	
96	The proposed solution shall identify vulnerabilities affecting AI frameworks, model dependencies and associated software components.	10	Select	0	
97	The proposed solution shall support AI governance by maintaining ownership, business criticality and lifecycle information for AI assets.	10	Select	0	
98	The proposed solution shall support AI asset search, filtering, tagging and classification.	10	Select	0	
99	The proposed solution shall automatically update AI-BOM records whenever AI models, datasets or dependencies are modified.	10	Select	0	
100	The proposed solution shall generate AI asset risk scores based on model exposure, dependency and business impact.	10	Select	0	

SBOM, CBOM, AI BOM AND QBOM

101	The proposed solution shall provide AI asset relationship visualization and dependency graphs.	10	Select	0	
102	The proposed solution shall provide APIs for AI-BOM integration with DevSecOps, GRC and enterprise asset management platforms.	10	Select	0	
103	The proposed solution shall maintain audit logs for AI-BOM creation, modification and access.	10	Select	0	
104	The proposed solution shall generate executive and technical reports for AI asset inventory, risk and compliance.	10	Select	0	
105	The proposed solution shall provide a centralized web-based management console for SBOM, CBOM and AI-BOM.	10	Select	0	
106	The proposed solution shall support Role-Based Access Control (RBAC) with granular administrative privileges.	10	Select	0	
107	The proposed solution shall support LDAP, Active Directory and Single Sign-On (SSO) integration.	10	Select	0	
108	The proposed solution shall provide secure REST APIs for integration with enterprise applications.	10	Select	0	
109	The proposed solution shall support integration with CI/CD and DevSecOps pipelines for automated BOM generation and updates.	10	Select	0	
110	The proposed solution shall integrate with vulnerability management, SIEM and GRC platforms.	10	Select	0	
111	The proposed solution shall support configurable dashboards for technical, operational and executive users.	10	Select	0	
112	The proposed solution shall support configurable reports in PDF, CSV and machine-readable formats.	10	Select	0	
113	The proposed solution shall maintain immutable audit logs for all user and administrative activities.	10	Select	0	
114	The proposed solution shall support High Availability (HA) deployment with automatic failover capabilities.	10	Select	0	
115	The proposed solution shall support Disaster Recovery (DR) deployment with secure data replication.	10	Select	0	
116	The proposed solution shall support encryption of all BOM data both at rest and in transit.	10	Select	0	
117	The proposed solution shall support configurable workflow, approval and notification mechanisms.	10	Select	0	
118	The proposed solution shall support scheduled, on-demand and event-driven discovery and reporting.	10	Select	0	
119	The proposed solution shall support secure import and export of BOM information using industry-standard formats and APIs.	10	Select	0	
120	AIBOM Solution can Scan a model file, report metadata.	10	Select	0	
121	AIBOM Solution should include base model info, for one file format (GGUF)	10	Select	0	
122	Solution should include model architecture for one file format (GGUF)	10	Select	0	
123	The Solution should Continue exploring more file formats, monitor regulation about AIBOM	10	Select	0	
124	The solution shall automatically discover cryptographic and quantum-related assets across on-premises, cloud, virtualized, containerized, and hybrid environments.	10	Select	0	
125	Applications, Servers, Databases, APIs, PKI, Certificates, HSMs, KMS, Containers, Kubernetes, Network Devices, VPNs, IoT, Cloud Services.	10	Select	0	
126	Automatically identify RSA, ECC, DSA, Diffie-Hellman, ML-KEM,ML-DSA AES, SHA, TLS, SSH, IPSec, PQC algorithms, and hybrid implementations.	10	Select	0	
127	Agent-based, Agentless, API-based, Scheduled, Continuous Discovery.	10	Select	0	
128	Maintain centralized QBOM repository with configurable metadata.	10	Select	0	
129	Discover relationships between applications, cryptographic libraries, certificates, protocols, APIs, and infrastructure components.	10	Select	0	
130	Maintain cryptographic library, protocol, certificate, and software version history.	10	Select	0	
131	Automatically identify quantum-vulnerable cryptographic implementations.	10	Select	0	
132	Identify assets containing long-term confidential data susceptible to future quantum attacks.	10	Select	0	
133	Assess readiness for migration to post-quantum cryptography.	10	Select	0	
134	Evaluate algorithm abstraction, hybrid support, dynamic algorithm replacement, and migration capability.	10	Select	0	
135	Detect hybrid deployments combining classical and PQC algorithms.	10	Select	0	
136	Generate migration plans based on business criticality and quantum risk.	10	Select	0	
137	Classify assets as Critical, High, Medium, or Low using configurable criteria.	10	Select	0	
138	Monitor inventory changes, algorithm updates, certificate lifecycle, and policy compliance.	10	Select	0	
C	Operations and Reporting				
139	The solution must offer an ability to generate audit ready reports for consumption of auditors.	10	Select	0	
140	The solution must offer a Role Based Access Control that limits the view into data as per the roles configured in the system.	10	Select	0	
141	The solution must offer ability to view data by the application for each role base don certain fields.	10	Select	0	
142	The solution must support role based access like Auditor, Application Owner , Security Admin etc.	10	Select	0	
143	The solution must be able to generate, schedule and deliver reports over email for executives on a prescheduled cadence.	10	Select	0	

Total	1500	0
-------	------	---

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

DNS SECURITY

DNS Security					
S.No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
A					
GENERAL					
1	The proposed solution must be fully cloud based Authoritative DNS solution providing low latency, reliable and secure DNS communication.	10	Select	0	
2	DNS Platform should be purpose-built exclusively to serve DNS traffic to avoid any inter-dependency on other solutions on the provider's platform. DNS Platform to have 1000+ POPs globally with multiple POPs in India as well.	10	Select	0	
3	Segmented Architecture design to handle both Performance and Availability aspects separately to ensure there are no performance lag or possibility of a DNS system failure.	10	Select	0	
4	DNS Platform should offer 100% Availability SLA, considering how important DNS availability is to Bank.	10	Select	0	
5	The solution must be built on global anycast technology	10	Select	0	
6	The solution must support low latency response time for DNS queries	10	Select	0	
7	Authoritative DNS services should be ISO 27001:2013 & ISO 27701:2019 compliant	10	Select	0	
8	Solution should support both primary and secondary DNS deployments	10	Select	0	
9	DNS Service must support following Record Types: 1) A IPv4 Address 2) AAAA IPv6 Address 3) AFSDB AFS Database 4) CNAME Canonical Name 5) DNSKEY DNS Key 6) DS Delegation Signer 7) HINFO System Information 8) LOC Location 9) MX Mail Exchange 10) NS Name Server 11) NSEC3 Next-Secure, Version 3 12) NSEC3PARAM NSEC3 Parameters 13) PTR Pointer 14) RP Responsible Person 15) RRSIG DNSSEC Signature 16) SPF Sender Policy Framework 17) SRV Service Locator 18) TXT Text	10	Select	0	
10	The DNS platform should be designed to avoid the known vulnerabilities and weaknesses associated with BIND architecture. The platform shall incorporate advanced security features at the non-BIND architectural level while still maintaining full compliance with DNS RFCs and IETF specifications.	10	Select	0	
11	Solution must provide static name server IP for each domain used by the Bank.	10	Select	0	
B					
DNS Solution - Security					
12	The DNS solution must support DNSSEC capability to secure DNS zones and records	10	Select	0	
13	DNS service must provide protection against DDoS attacks directed at Bank's DNS Infra on their platform.	10	Select	0	
14	DDoS Protection for DNS Solution should be bundled as part of the overall solution & there should be no separate or extra fees for handling DDoS attacks. Bank must not be billed for any Volumetric Attack Traffic at DNS Layer.	10	Select	0	
15	If there is any DNS or DDOS attack on DNS Service, service provider should have necessary detection & mitigation mechanism to ensure 100% Availability and no disruption to bank services.	10	Select	0	
16	DNS service must provide DNSSEC with 'Sign & Serve' option. DNS Service provider must handle Key Rotation for DNSSEC and Bank team should be offloaded of the task of Key Rotation. DNSSEC is required to protect Bank's DNS Infrastructure for emerging DNS based threats and DNS Service Provider should handle complete DNSSEC related key management and offer the same as a service to Bank.	10	Select	0	
17	Solution Should offer protection for DNS attacks, such as DNS Security – DDoS DNS attack protection UDP/TCP/ICMP Flood DNS hijacking DNS amplification DNS reflection DNS Cache poisoning DNS NxDomain Attack	10	Select	0	
18	The solution must have comprehensive volumetric DNS DDoS Protection with minimum 1 Tbps mitigation capacity	10	Select	0	
19	The solution must allow users to create policy rules to block DNS resolution based on geographic location or IP prefix	10	Select	0	
20	Rate-Limiting for DDOS to drop even a single IP should be available as part of the solution.	10	Select	0	
21	During DDOS, DNS Security solution should have capabilities to apply positive security model and restrict DNS requests to a list of known-good DNS resolvers only.	10	Select	0	
C					
Technical Specification - Cloud Based Load Balancing Solution - GSLB					
22	Should be an Cloud & DNS based traffic load balancing solution that integrates with existing DNS solution.	10	Select	0	
23	Solution should offer 100% Availability SLA for Cloud Based Load Balancing Solution to ensure no traffic is dropped.	10	Select	0	
24	Should Support Active - Active Load balancing across multiple DC/DR	10	Select	0	
25	Should Support Active - Passive Load balancing to handle Primary & Secondary sites	10	Select	0	

DNS SECURITY

26	Should Support Weighted Load balancing e.g. 20/80 or 30/70, etc. Traffic split between sites	10	Select	0	
27	Should provide IP Intelligence to redirect the traffic based on geography	10	Select	0	
28	No Limitations on the traffic or number of queries handled by the traffic Management solution	10	Select	0	
29	No commercial impact due to the number of queries or traffic volume handled by the traffic Management solution	10	Select	0	
D	DNS & GSLB Web Management				
30	The solution must provide a management console (GUI) for managing DNS records	10	Select	0	
31	The solution must also provide API for creating, modifying, and deleting DNS records	10	Select	0	
32	The solution must provide Role Based Access Control (RBAC)	10	Select	0	
33	The solution must enforce Two Factor Authentication for registered users	10	Select	0	
34	Bank must get Web Portal based access for configuration of DNS service	10	Select	0	
35	Bank must get facility to whitelist Bank IP Addresses to Management Web Portal. This is to ensure that any configuration changes are done from Bank network only	10	Select	0	
36	Bank must get facility to enable 2FA for Management Web Portal. This will provide additional layer of security for Bank from configuration and reporting perspective	10	Select	0	
37	DNS Service provider should provide unified portal to monitor complete DNS security related tasks like configuration, reporting, billing etc.	10	Select	0	
E	Service and support SLA				
38	DNS Service Provider OEM must have their own First Party NOC, SOC, and Technical Support Centre (24 x 7 x 365) in India. This is to ensure that DNS Service provider has significant commitment towards India region. Bank may request to visit these centers for verification of support & services centers.	10	Select	0	
39	The solution must come with 24x7 OEM Support for break and fix issues	10	Select	0	
40	The solution must show uptime status on GUI and must send monthly uptime reporting via email.	10	Select	0	
41	The service shall have 24x7 Service hour support for 365 days and a ticketing mechanism to support time bound escalation and resolution support.	10	Select	0	
42	Provide one-time detailed Training to Bank technical team to manage the solution effectively	10	Select	0	
F	Fixed Pricing Model				
43	Pricing for DNS or GSLB Solution must not be dynamic or traffic consumption based e.g. Based on DNS queries or traffic served. There should not be any extra cost to absorb DDoS attack traffic handled by the DNS platform for Bank DNS Zones or GSLB. Pricing should be predictable & Flat based on the number of DNS zones or GSLB configurations as per Bank's requirement.	10	Select	0	
44	20 Domains of PSB are to be considered for the purpose of sizing	10	Select	0	
Total		440		0	

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

CASB

CASB					
S.No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
	If any component of the proposed solution is hosted on a cloud platform, indicate whether the Product OEM/Cloud Service Provider (CSP) has submitted CSP compliance functional specifications and supporting documentation demonstrating compliance with all applicable requirements of this RFP. If the dropdown is not selected, the product will be considered NON COMPLIANT.		Select		
1	The Proposed CASB Solution should be available in India, no DLP & threat scanning should not happen outside India DCs. The Proposed solution's all components (on-prem HW or Software if any) should connect to management plane within India for any kind of monitoring/health checks of components. This is applicable for user and server segment traffic as well and will be strictly enforced as per RBI/DPDP rules & under no condition it will allow monitoring/meta data to be stored/copied outside india	10	Select	0	
2	The proposed solution must have single light weight user agent <50MB and supported on Windows, MAC, Linux, iOS, chromeOS, windows terminal server 2022, Citrix virtual apps & desktops and azure virtual Desktops	10	Select	0	
3	The proposed solution should have CSA STAR, SOC 2, CIS, ISO 27001, ISO 27017, ISO 27018 certification and must be a part of Microsoft Active Protections Program (MAPP)	10	Select	0	
4	User License for any proposed component must not be limited by any bandwidth or data cap and licensing should not depend on Bandwidth consumed by users.	10	Select	0	
5	The solution must have granular role based access control (specific admins as like for Threat, data protection and Access Control should be able to monitor and control only their specific policies and reportings).	10	Select	0	
6	The proposed solution shall be cloud-native, support Zero Trust principles, provide secure access to web, cloud, and private applications, and demonstrate proven enterprise deployments.	10	Select	0	
7	The Solution must have a native MFA integration for the Admin Accounts created locally on the Admin Portal to ensure secured and authenticated access and it must be accessible from only Authorized Public IP	10	Select	0	
8	The deployment of the solution must be supported both agent and agentless mechanism so that customer can select/choose respective method to route traffic to SSE platform basis on their environment/ requirement. The solution must have below mechanism for forwarding traffic agent-based, IP Sec Tunnel, GRE Tunnel, Explicit Proxy / PAC Based	10	Select	0	
9	The offered solution shall support the following User Authentication methods: • Microsoft Active Directory, • LDAP • SAML • ADFS	10	Select	0	
10	The solution should have direct OEM 24x7x365 Support with 30 Minutes response time for P1 tickets from day one	10	Select	0	
11	The proposed solution shall provide high availability with documented service availability commitments and optimized traffic routing to ensure consistent user experience.	10	Select	0	
12	The proposed solution must be able to ingest or share IOC with other security vendors and shoule be able to forward logs to On-premise/SIEM	10	Select	0	
13	The proposed solution shall provide configurable log retention, search, reporting, and audit capabilities through the management console. Log retention duration shall be configurable in accordance with the Bank's regulatory, operational, and compliance requirements.	10	Select	0	
14	The Proposed Inline CASB solution must not have a single point of failure and should have seamless failover transparently to secondary site's (running with same full scale & specified features) if primary site goes down. All features should be available from Day1	10	Select	0	

CASB

15	The Proposed solution should have capable to setup policy based on: End-User Device Posture Assessment: a. Posture Check including Certificate check, Domain check, AV agent check, customer's Custom apps check, process and registry check on endpoints. b. The Posture assessment must be periodic in nature and repeat in every 15 minutes or less to ensure continued compliance	10	Select	0	
16	The offered platform should be TLS1.3 , HTTP/2 enabled right from day1	10	Select	0	
17	The solution must operate in a full-proxy architecture and should perform 100% SSL inspection at scale. The solution must detect and block malware passing in an encrypted HTTPS tunnel. This must include the capability to Inspect the Web Traffic sent by CLI Commands (For ex. S3) and Thick Clients like MS Teams to enable secured transactions without any user experience issues from Day 1.	10	Select	0	
18	The proposed solution must have capability to enforce granular advance activity control as mentioned below: a. Webmail Category: Upload, Download, & Attach,Send, b. File Sharing / Cloudstorage category: Upload, Download, & Post. c. Collaboration Category: Upload, Download, & Post d. Generative AI: AI Post, AI Response, Attach, generate etc.	10	Select	0	
19	The solution must include an Agentic Broker capability that provides centralized visibility and control over AI agents operating within the environment, ensuring all agent-to-agent and agent-to-data interactions are monitored, governed, and secured in real time. This must be available with same agent and same platform with additional licenses as required in future	10	Select	0	
20	The Propsoed solution must also let admin create their own custom categories for filtering and it should have features like safe search, silent ad blocking, and a way to quickly rate pages that don't have a rating yet. Plus, it should check a website's category and change its rating if needed, all while watching the web traffic based on these content types	10	Select	0	
21	Proposed solution must have capability to apply control to specific file type and size for a user, location, and/or destination based on policy	10	Select	0	
22	The Propsoed solution should Detect data movement, insiders threat, and acceptable use policy based on corporate vs 3rd Party vs Personal instances of a SaaS apps and IAAS	10	Select	0	
23	The solution must support the validation of internet websites with an untrusted server certificate. It must support OCSP (Online Certificate Status Protocol) to obtain the revocation status of an application/server with an untrusted certificate and take the required action, which includes allowing, blocking, or passing through the access with a warning to the user.	10	Select	0	
24	The solution should support real-time visibility for minimum 70,000+ cloud applications with dynamic risk score based on Cloud Security Alliance Standards. The solution must be able to report the security compliances and certifications achieved by these apps.	10	Select	0	
25	The solution must provide the granular visibility and control on Azure, AWS allowing monitoring and management of cloud resources within the environment. It must support the activity control like activate, connect, terminate, stop, start, shutdown etc for IAAS/PAAS resources.	10	Select	0	
26	The solution must provide coach Users: Provide automated and customized coaching messages to educate and guide users regarding undesirable cloud activities and the risks associated with uploading sensitive data to unmanaged cloud services.	10	Select	0	
27	The Inline CASB Policies criteria must have the following parameters - Source IP address, OS Family, Browser type, device classification, source country, source Public IP, Cloud Applications Categories and policies can be defined by time intervals means during working hours users will get different policies and during non-working hours different policies will be applied	10	Select	0	

CASB

28	The solution must have the below threat protection modules to protect against Internet based Threats: a. Anti-Malware Engine (for Viruses, Malwares, & Trojans) b. Web IPS (for Advanced Threat Protection against C&C Servers, DGA botnet attacks, malicious active content, P2P anonymisers) c. Inline Sandbox which leverages AI and Machine Learning based analysis and Patient Zero infections across PE (portable executable) file types..	10	Select	0	
29	The proposed solution must have integration with Third Party Threat feeds and the capability for bi-directional IOC exchange (MD5,SHA.urls etc) through custom rest APIs. The solution must be able to add manual IOCs (MD5 and hashes) directly from admin console in real time to minimise risk.	10	Select	0	
30	The solution must be able to inspect & block multilayer zipped / compressed files.	10	Select	0	
31	The proposed solution must provide open threat intel exchange platform to integrate with customer environment existing security stack such as EDR Solutions, Threat intel exchange solution, SIEM solutions, SSO solutions etc.	10	Select	0	
32	The solution should have capability to provide UEBA profiling based on the below parameters: A. Data exfiltration: Capability to detect and alert in case the user downloads file from a corporate instance of SaaS app like OneDrive and transfers the files to Personal Account. B. Location Awareness: Capability to detect and alert in case the geolocation of the user changes abruptly and in a non-realistic fashion (for ex. India Users suddenly logged in from Russia) C. Bulk Upload and download: Capability to detect and alert in case the User Uploads or Downloads files from Corporate Applications in Bulk. D. Bulk Deletion of files: Capability to detect and alert in case the User Deletes files in Corporate Applications in Bulk. E. Login failures: Capability to detect and alert in case the User makes multiple and continuous failed login attempts to a corporate application	10	Select	0	
33	Solution must be able to determine the Instance/Tenant of Internet/SaaS Applications being accessed and enforce dedicated Access Control and Data Protection Policies for each Tenant/Instance of the same Application. This capability must be supported across hundreds of Internet/SaaS Applications including MS O365 where the Solution must decrypt the SSL traffic destined to O365 Apps.	10	Select	0	
34	The Solution must be able to enforce policies based on Granular Activity Control for all well known SaaS/IAAS Applications. The activities like Terminate, stop, publish, shutdown, share, send, search, reject, register, reboot must be supported for IAAS services like Azure and AWS	10	Select	0	
35	The Solution must support CLI (AWS S3 bucket and WebUI for Specific Services: It is essential to have command-line interface (CLI) and web user interface (WebUI) capabilities for specific services, enabling efficient management and control	10	Select	0	
36	The solution must be able to enforce granular activity based policies on users trying to access official Internet Apps (O365, Google and more) via an Unmanaged Device like Tablet or Personal Laptops.	10	Select	0	
37	The solution must provide the granular visibility and control on Azure, AWS allowing monitoring and management of cloud resources within the environment. The solution must support data protection on Azure blob storage, S3 buckets. The solution must support the DLP capabilities accessing S3 buckets via CLI.	10	Select	0	
38	The solution must provide the granular Visibility and Control on Generative AI applications like (ChatGPT,MS copilot etc. Solution must be able to determine the Instance/Tenant of Generative AI applications being accessed and enforce dedicated Access Control and Data Protection Policies for each Tenant/Instance of the same Applications.	10	Select	0	
Total		380		0	

AI SECURITY					
S.No.	Required Functionalities/Features	Maximum Marks	Compliance (S/C)	Calculated Score	Remarks
AI Security					
1	The proposed solution must provide Shadow Discovery of Gen AI apps running in the customer environment, differentiate private vs Public instances, restrict sensitive data upload to public-instance Gen AI apps, and maintain a curated catalog of Gen AI applications and MCP servers with automated risk scoring based on security attributes, data handling practices, and compliance.	10	Select	0	
2	Continuously discover and risk-rate all GenAI, LLM and AI-copilot applications in use across the organization, including unsanctioned ("Shadow AI") tools, without requiring prior app-specific integration.	10	Select	0	
3	Solution should have a common dashboard for the discovered agent, models, AI apps and MCP for the central view.	10	Select	0	
4	Inspect and control data leaving the organization through prompts, file uploads and pastes into AI applications in real time, before the data reaches the AI provider.	10	Select	0	
5	Allow administrators to permit lower-risk activities (e.g., 'ask a question') while blocking higher-risk activities (e.g., 'upload file', 'paste source code', 'share screen') within the same AI application.	10	Select	0	
6	Maintain and auto-update a cloud/AI application risk-rating database covering data handling, certifications and known incidents for thousands of AI/SaaS apps.	10	Select	0	
7	Apply DLP, threat protection and access control to AI traffic in a single inspection pass to minimize latency and avoid repeated TLS decrypt/re-encrypt cycles.	10	Select	0	
8	Detect anomalous AI usage patterns (e.g., abnormal volume of prompts, unusual data types submitted, off-hours usage) and trigger adaptive risk response.	10	Select	0	
9	Enforce AI security policy consistently for corporate-managed devices, BYOD and remote/unmanaged endpoints via a cloud-delivered security service edge.	10	Select	0	
10	The solution must include an Agentic Visibility and Control capability providing centralized visibility and control over AI agents, ensuring all agent-to-agent and agent-to-data interactions (including via MCP) are monitored, governed, and secured in real time — with granular control to permit AI agents to "Read" from enterprise data sources while strictly blocking "Update"/"Delete" operations. This must be available on the same agent/platform with additional licenses as required in future.	10	Select	0	
11	The solution must provide granular visibility and control on Generative AI applications (ChatGPT, MS Copilot, etc.), determine the Instance/Tenant being accessed, and enforce dedicated Access Control and Data Protection Policies per Tenant/Instance of the same application.	10	Select	0	
12	The proposed solution should not be dependent on any on-premise device/NGFW to provide SaaS or Gen AI app activity controls such as upload, share, post, AI post, comment, send, create, modify, download, etc., nor by any DLP solution for data at rest it has to be inline	10	Select	0	
13	The proposed solution should provide DLP-level controls to block and monitor data exfiltration over Gen-AI apps, including detailed user coaching that redirects users to corporate Gen AI apps, with an option for users to justify business use case before interacting further.	10	Select	0	
14	The proposed solution should provide detailed visibility, granular activity controls, and protection for users interacting not only with standalone Gen-AI applications but also with Embedded AI on websites and applications.	10	Select	0	
15	The proposed solution should inspect Model Context Protocol (MCP) servers for bi-directional data sharing between apps, agents, and LLMs (including via CLI), and provide visibility/granular activity controls for public MCP servers — detecting and inspecting message types such as CallToolRequest/Result, CreateMessageRequest/Result, Elicit Result, GetPromptRequest/Result, Initialize Request/Result, ListPromptsResult, ListResourceResult, ListToolsResult, ReadResourceRequest/Result, etc. — for real-time policy enforcement, DLP, and threat scanning, in accordance with the Bank's performance and scalability requirements	10	Select	0	
16	The solution must provide a real-time inspection engine capable of detecting and mitigating Generative AI-specific threats, including prompt injection, jailbreaking, and leakage of copyrighted or patented material/	10	Select	0	
17	The Proposed solution should have capable to setup policy based on: End-User Device Posture Assessment:				
17.1	Posture Check including Certificate check, Domain check, AV agent check, customer's Custom apps check, process and registry check on endpoints.	10	Select	0	
17.2	The Posture assessment must be periodic in nature and repeat in every 15 minutes or less to ensure continued compliance"	10	Select	0	
18	The offered platform should be TLS1.3, HTTP/2 enabled right from day1	10	Select	0	
19	This must include the capability to Inspect the Web Traffic sent by CLI Commands (For ex. S3) and Thick Clients like MS Teams to enable secured transactions without any user experience issues from Day 1.	10	Select	0	
AI Guardrails					
1	The proposed solution should provide detailed visibility, granular activity control, and protection for both Gen-AI prompts and responses — blocking content that bypasses LLM safety protocols, constitutes prompt injection/jailbreaking attempts, or is harmful/ hateful/ biased/ inappropriate/ risky — with policies mapped to MITRE ATLAS and OWASP Top 10 for LLMs.	10	Select	0	
2	Inspect prompts submitted to any AI application in real time for sensitive data (PII, PCI/PAN, credentials, source code, financial records) prior to submission.	10	Select	0	
3	Inspect AI-generated responses in real time for data-leakage, policy violations or disallowed content before it reaches the end-user.	10	Select	0	
4	Provide pre-built, tunable data identifiers relevant to banking (account numbers, SWIFT/IFSC/routing codes, card PAN, KYC data) usable directly in AI guardrail policy.	10	Select	0	
5	Solution should enforce content moderation guardrails for responsible AI usage by detecting and protecting from many categories of AI prompts and responses, such as inappropriate/harmful content, hate, bias, weapons as well as copyright or patented data that expose a new risk vector for organizations.	10	Select	0	

AI Security, Guardrail and Gateway

6	The system must support advanced detection beyond pattern matching, using semantic analysis to identify sensitive content (e.g., hate speech, crimes, sensitive data requests) with adjustable confidence thresholds.	10	Select	0	
7	The platform must provide granular visibility and policy control across a broad catalog of GenAI applications, including standalone apps and embedded assistants.	10	Select	0	
8	The solution must have the ability to differentiate and apply unique policies to specific AI activities — Prompt/Post (outbound), Response (inbound), File Upload/Attach (data sharing), and AI-generate actions	10	Select	0	
9	The proposed solution should support over 30 languages (including East Asian and European) for AI inspection.	10	Select	0	
10	The solution must integrate AI-specific guardrails with deep-content inspection technologies like OCR, to protect sensitive data within screenshots/images uploaded to LLMs.	10	Select	0	
11	The solution must provide the capability to block or allow the download of MCP server code from public repositories (e.g., GitHub) based on repository age, stars, or security reputation.	10	Select	0	
12	The solution must have the capability to inspect and apply policy to custom HTTP headers used in MCP communications, to prevent data exfiltration through non-standard channels.	10	Select	0	
13	The AI security layer must integrate with enterprise-grade DLP to prevent upload of PII, PCI, or PHI into LLMs, while providing real-time feedback to educate users on safe AI usage. The solution should support real-time visibility for cloud applications with dynamic risk score based on Cloud Security Alliance Standards. The solution must be able to report the security compliances and certifications achieved by these apps.	10	Select	0	
AI Gateway					
1	Provide a centralized AI Gateway that acts as the single inspection and policy-enforcement point for all outbound and internal AI/LLM traffic, including agentic calls.	10	Select	0	
2	Automatically maintain an inventory and control of all Model Context Protocol (MCP) servers and tools connected to, or invoked from, the enterprise environment.	10	Select	0	
3	Enforce identity-based authentication and least-privilege authorization for every MCP tool/resource call, consistent with zero-trust principles.	10	Select	0	
4	Inspect the parameters and payloads of MCP tool calls for sensitive data or policy violations before the call is executed against the target system.	10	Select	0	
5	Maintain an administrator-defined allow-list/deny-list of approved MCP servers and specific tools, enforced at the gateway.	10	Select	0	
6	The Proposed Solution should be available in India, no DLP & threat scanning should not happen outside India DCs.	10	Select	0	
7	The Proposed solution's all components (on-prem HW or Software if any) should connect to management plane within India for any kind of monitoring/health checks of components. The proposed solution should have CSA STAR, SOC 2, CIS, ISO 27001, ISO 27017, ISO 27018 certification and must be a part of Microsoft Active Protections Program (MAPP)	10	Select	0	
8	Solution is available as a lightweight virtual appliance for public cloud deployments in AWS, or private cloud deployments with VMware ESXi.	10	Select	0	
9	Solution Operates a software defined gateway to intercept and govern API traffic , internal applications , autonomous agents and private hosted LLM.	10	Select	0	
10	Solution Provides a unified API entry point to manage interactions across multiple providers, including OpenAI, Google Gemini, Anthropic Claude, and custom models following the API schema for these models	10	Select	0	
11	Solution use only authenticated agents for the communication , by using token from AI gateway	10	Select	0	
12	The solution must have the ability to differentiate and apply unique policies to specific AI activities — Prompt/Post (outbound), Response (inbound), File Upload/Attach (data sharing), and AI-generate actions for the AI Gateway	10	Select	0	
13	The proposed solution should support over 30 languages (including East Asian and European) for AI inspection.	10	Select	0	
14	The solution must integrate AI-specific guardrails with deep-content inspection technologies like OCR, to protect sensitive data within screenshots/images uploaded to LLMs.	10	Select	0	
15	The solution must provide the capability to block or allow the download of MCP server code from Private MCP	10	Select	0	
16	All AI Gateway has to be native managed by common AI Security and Guardrails in Line with unified agent and Management	10	Select	0	
General					
1	The proposed solution should provide the following features and capabilities:				
1.1	Unified policy fabric for Data Protection + AI Security with policies and consolidated logging with granular control per acitivity .	10	Select	0	
1.2	Content + Context + Intent based risk analysis and policy decisions.	10	Select	0	
1.3	Discovery of Embedded AI browser extensions, plug-ins and connectors using AI with Agent and Agentless	10	Select	0	
1.4	Enterprise-wide protection across Email, SaaS, Files, Endpoints and AI prompts.	10	Select	0	
1.5	Configurable enforcement actions including Content Moderation, Coach in addition to Block/Monitor.	10	Select	0	
1.6	Browser and Endpoint agents distributable through MSI packages/MDM.	10	Select	0	
1.7	Agent based controls with activity controls (Visit, Copy, Paste, Share, Upload, Post).	10	Select	0	
1.8	Detection and control of non-browser AI interactions (Cursor, Claude Desktop, CLI, local AI tools, etc.) with Data and Threat , Guardrails	10	Select	0	
1.9	Protection against Tool/Function Hijacking and adversarial inputs.	10	Select	0	
1.10	Detection of insecure AI code assistant recommendations (secret leakage, insecure code patterns).	10	Select	0	
1.11	AI Command Center or Security Posture Management dashboard with Scoring	10	Select	0	
1.12	Compliance-ready dashboards.	10	Select	0	
1.13	Context-aware user coaching with safer alternatives.	10	Select	0	
1.14	Real-time enforcement with minimal impact on user experience.	10	Select	0	
1.15	AI-powered classifiers using semantic understanding instead of only pattern matching.	10	Select	0	
1.16	AI Central Command Center for the view of Inventory including models, agents, MCP servers, tools, hooks, repositories and permissions.	10	Select	0	
1.17	Single control plane for multiple LLM providers (like Azure OpenAI, Bedrock, Vertex AI, Anthropic, etc.)	10	Select	0	
1.18	API or Inline compatibility with OpenAI, Anthropic, Bedrock and Vertex AI schemas without application code changes.	10	Select	0	

AI Security, Guardrail and Gateway

1.19	Separate policy actions for Request and Response paths.	10	Select	0	
1.20	Ability for the Bank to create its own semantic detectors without vendor professional services.	10	Select	0	
1.21	Custom prohibited-topic detection models.	10	Select	0	
1.22	Secure API key abstraction through AI Gateway (application never stores provider keys).	10	Select	0	
1.23	Policy-based model routing/weighted load balancing/automatic failover and token/request rate limiting.	10	Select	0	
1.24	AI Gateway dashboards for request, response and token consumption.	10	Select	0	
1.25	Centralized System Prompt Repository injected by the Gateway.	10	Select	0	
1.26	Detailed operational dashboards and exportable reports (tokens, prompts, models, providers, users, streaming, tool usage).	10	Select	0	
1.27	Native SIEM/SOC integration	10	Select	0	
1.28	Unified management of Endpoint Sensors, LLM Gateway and MCP Gateway.	10	Select	0	
1.29	Governed MCP Discovery and control supporting pre-built and custom MCP servers.	10	Select	0	
1.30	Control on MCP server capabilities (Tools, Resources, Prompts, Schemas).	10	Select	0	
1.31	Gateway-terminated authentication for MCP with OAuth/Dynamic Client Registration/API Keys.	10	Select	0	
1.32	Complete logging of MCP protocol payloads, tool invocations and policy decisions.	10	Select	0	
1.33	Enforcement across MCP protocol primitives (initialize, tools/list, tools/call, resources/read, prompts/get, etc.).	10	Select	0	
1.34	Request-path and Response-path inspection for MCP traffic.	10	Select	0	
1.35	Solution should support AI Access graph for the users , agent and MCP	10	Select	0	
1.36	Tamper-evident audit logs with API-based retrieval.	10	Select	0	
1.37	Gateway latency and scalability requirements.	10	Select	0	
1.38	Mapping Red Team findings to OWASP LLM Top 10, MITRE ATLAS, Agentic AI and NIST AI RMF.	10	Select	0	
1.39	Selective re-testing of attack categories.	10	Select	0	
1.40	Exportable Red Team reports with raw prompts and responses.	10	Select	0	
1.41	Native integration of Guardrails within AI Gateway	10	Select	0	
Total		900		0	

Cloud Solution

S.No.	Minimum 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. 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	Requiste provisioning of network infrastructure (including switches, router, firewalls, and load balancers) to ensure accessibility of the servers as per defined SLA's. 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.			
4	The solution shall meet Bank-defined RPO/RTO and resilience requirements irrespective of the replication technology adopted.			
5	Data Centers/hosting facilities used by the solution should be minimum Rated 3 of TIA940 or Tier 3 of Uptime Institute or any other equivalent certification			
6	Where the solution is hosted, CSP should be empaneled with the Ministry of Electronics and Information Technology (MeiTY)			
7	Perform regular tech refreshes, patch management and other operations of provisioned infrastructure that is in the scope under this RFP.			
8	The Solution provider/CSP shall provide bank with the necessary logs for the services for security monitoring and incident alert management.			
9	OEM shall remain solely responsible for patching, infrastructure operations, logging, interoperability, API security, portability and migration support irrespective of backend infrastructure ownership.			
10	OEM shall ensure compliance of the complete proposed solution & platform with RBI, CERT-In, CSCRF, DPDP Act, IT Act, MeiTY and all applicable regulations throughout the contract period.			
11	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.			
12	The Solution provider 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.			
13	The CSP shall ensure to protect confidential information from unauthorized disclosure and use			
14	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.			
15	If Indian government demand is received for any data, the process mentioned below has to be followed:			
15.1	Disclosure of data of any kind on legal/statutory compulsion should be done only after obtaining concurrence from the Bank.			
15.2	Resist illicit demands that are invalid which are not permitted by the Indian Government or Indian IT Law or any other Indian Regulatory Authorities.			
16	Solution provider should have capability to provide Alerts & Monitoring interface. Solution should support Remote Administration for administrators			
17	Solution provider should have Capability to integrate with the bank's authentication servers (LDAP/ADFS etc.) and Integration with applications using API.			
18	The cloud infrastructure should have presence in at least 2 cities in India in different SEISMIC Zone			
19	Any data transmission and storage should be encrypting data both at rest and in transit with SSL/TLS (minimum TLS 1.2).			
20	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.			
21	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.			

Cloud Solution

22	The proposed solution should not mandate any minimum number of users for any service uptime calculations.			
23	The proposed solution should also have Service level commitments for virus detection and blocking, spam effectiveness, false positives as well as email delivery.			
24	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.			
25	The personnel controls are to be in place to provide a logical segregation of duties.			
26	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.			
27	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.			
28	Secure Data Deletion: Require that Bidder offer a mechanism for reliably deleting data on Bank's request ensuring no data reminiscence			
29	Solution provider 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.			
30	Solution provider 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.			
31	Solution provider should provide right to audit as similar what Bank is having with shared data centers in India. In addition:			
31.1	a. Bank's data should not cross Indian geographical boundaries (physically or logically).			
31.2	b. Bank must have "Rights to Audit" the compliance with the CSP agreement including rights of access to the CSP's premises where relevant records and Bank's data is being held.			
31.3	c. Audit rights for the Bank or its appointed auditor (nominee) or regulators should be integral clause in agreement.			
31.4	d. Integration of all devices with Bank's SOC, SIEM & other security solution for monitoring.			
31.5	e. Bank should have access/ monitoring mechanism for Privilege user access (of CSP) to cloud based systems.			
32	a. 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.			
33	b. 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.			
34	c. 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			
35	d. The bidder shall provide the artifacts, security policies and procedures demonstrating its and CSP's compliance with the Security Assessment and Authorization requirements.			
36	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 at all locations			
37	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.			

Cloud Solution

38	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.			
39	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			
40	The bidder should ensure Data segregation, confidentiality, privacy controls setup in line with the bank's requirement			
41	In case of Exit/ change, Solution provider to ensure the following while formulating the exit plan			
41.1	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.			
41.2	ii. Detail out procedures to be used for deletion/destruction of data in a manner that data is rendered irrecoverable.			
41.3	iii. Independent audit for testing effectiveness of secure data removal, such that data is rendered permanently inaccessible. (Including any backup or distributed online media).			
41.4	iv. Transferability of cloud outsourced services to a third party, another CSP or on premise to the Bank for continuity of service.			
41.5	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.			
42	Cloud architecture shall account for and shall be submitted by bidder regularly at periodic interval to bank:			
42.1	a. Type of workload,			
42.2	b. Requirements of availability and resiliency,			
42.3	c. Security,			
42.4	d. Authentication,			
42.5	e. Performance,			
42.6	f. Operations and management.			
42.7	g. Logical segregation			
43	Security has been implemented at all layers i.e., Physical, Network, Data, Application, etc., of cloud architecture with multiple security controls.			
44	Bank's data should be isolated from other customers, to avoid comingling of data, in case of multi-tenancy.			
45	Cloud workload is protected against network-based attacks by implementing controls such as:			
45.1	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.).			
45.2	A dedicated security network segment (landing segment) shall be implemented for terminating all ingress traffic to the cloud.			
45.3	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.			
45.4	Micro Segmentation shall be implemented on the cloud.			
45.5	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.			
45.6	Direct network connection with cryptographic controls shall be implemented to secure the traffic between the cloud and on-premises environment.			
46	Implement principle of selective privileges and impose segregation of duties with appropriate access and authorization:			
46.1	To manage access rights to cloud services by the Bank's users, the CSP should provide user access management functions to the Bank.			
46.2	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.			
46.3	Multifactor authentication shall be implemented for user access to critical workloads and for all privileged access on the cloud.			
46.4	Users with privileged system access shall be clearly defined and regular user access reviews, at least once every three months, shall be conducted.			
46.5	Remote access by administrators and privileged users to the cloud environment over the Internet, shall not be permitted.			

Cloud Solution

46.6	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.			
46.7	Solution provider /Cloud Service Provider/ Cloud Management Team should not have access to any application data of the Bank.			
46.8	Conditional access should be implemented for privileged users.			
46.9	Legacy authentication protocols should be disabled.			
44.10	A granular access control policy should be implemented for access to any cloud resource.			
47	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.			
47.1	a. Critical/ sensitive data including PII/ SPDI, card holder data or account numbers shall be masked or encrypted.			
47.2	b. Bank shall have an option to implement 'Bring Your Own Key' as and when required.			
47.3	c. In case cloud based HSM is used, it should meet the FIPS 140-2 Level 3 and above criteria.			
47.4	d. HSMs and other cryptographic material should be stored on segregated secure networks with stringent access controls.			
47.5	e. In case CSPs/Solution provider 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.			
48	Retention of Bank's data on the cloud shall be in accordance with the extant guidelines of Bank's Data Retention Policy.			
49	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			
50	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.			
51	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.			
52	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			
53	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.			
54	File integrity monitoring should be implemented in order to ensure authenticated changes and to detect unapproved changes to files.			
55	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.			
56	Mechanism shall be implemented to detect service faults or outages in the cloud environment.			
57	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, Solution provider or CSP's plans should be shared with the Bank			
58	Change/Configuration management procedures shall be aligned with the Bank's Change Management policy, including change request, approval procedures and notification mechanism.			
59	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).			
60	Secure configuration settings related to OS/ database/ network devices/ virtual machines/ middleware should be implemented as per Bank's SCD or equivalent hardening guidelines.			
61	The cloud environment should follow the Bank's logging and monitoring policy.			
62	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.			
63	All logs of assets related to Bank's subscription/ tenant should be integrated with the Bank's SOC.			

Cloud Solution

64	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			
65	Roll-out / phasing-out of applications to / from cloud should follow the Data Migration Policy of the bank.			
66	For secure deletion/destruction of data:			
66.1	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.			
66.2	b. Do not use CE if it is unknown whether sensitive data was stored on the device without being sanitized prior to encryption.			
67	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.			
68	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.			
69	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.			
70	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.			
71	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			
72	Information security incident management process shall be established to discover, report, respond and prevent information security events and weaknesses effectively by Solution provider and CSP			
73	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.			
74	Requirements for forensic investigation including mechanism for acquisition of log data from CSP should be documented and reviewed & approved by bank.			
75	Bidder shall provide reasonable access to necessary information to assist in any Forensic investigation arising due to an incident in the cloud			
76	The IS controls' implementation should cover all locations that support Bank's data storage and/ or processing requirements.			
77	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.			
78	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			
79	Bidder should deploy Active Directory (AD), Single Sign On (SSO) and strong Password Policy for End point and application access			
80	Proper access control is to be defined for protecting PSB data and access to the Data is strictly on Need-to-Know Basis			
81	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			
82	Bidder confirms and agrees the following:			
82.1	Right to audit to PSB with scope defined.			
82.2	Right to recall data by PSB.			
82.3	System in place of taking approvals for making changes in the application.			
82.4	Regulatory and Statutory compliance at vendor site.			
82.5	IT Act 2000 & its amendments, and other Acts/Regulatory guidelines			
82.6	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.			
82.7	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.			
83	CERT IN Empaneled auditor report's is required for the following:			
83.1	Solution provider 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			

Cloud Solution

83.2	Solution provider follows the best practices of creation of separate network zones (VLAN segments) for Production and non-Production such as UAT			
83.3	Internet access is restricted on: Internal servers, database servers, Any other servers			
83.4	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.			
83.5	Solution provider has processes in place to permanently erase PSB data after processing or after a clearly defined retention period			
83.6	Log generation, storage, and review process to confirm whether proper log generation, storage, management, and analysis happens			
83.7	Whether the CSP/Solution provider has witnessed any security or privacy breach in the past 2 years			
84	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.			
85	Data should not be allowed to be downloaded or to prepare copies unless explicitly approved by bank.			
86	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.			
87	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.			
88	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			
89	Solution provider should ensure proper log generation, storage, management and analysis happens for the 3rd Party/Vendor application (including DFRA & access logs)			
90	Solution provider should have captive SOC or Managed Service SOC for monitoring their systems and operations			
91	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			
92	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.			
93	Rules are implemented on Firewalls of the 3rd Party/Vendor environment as per bidder approved process and rules & process are reviewed periodically.			
94	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			
95	Bidder should have in place procedures for emergency changes, including the roles and responsibilities, and that shall be documented.			
96	Mechanism shall be implemented for apprising details of sub-contracting of workload and periodically notifying changes in sub-contracting by Solution provider to Bank			
97	Solution provider or CSP should have Risk Framework in place for cloud adoption shall include but not be limited to following checks:			
97.1	Type of service being outsourced			
97.2	Application criticality			
97.3	Classification of data			
97.4	Cloud service model			
97.5	Cloud deployment model			
97.6	Data localization requirements and Laws affecting cross-border data transfer and storage			
97.7	Legal, regulatory and compliance requirements			
97.8	Data availability and recovery requirements			
97.9	Data recovery in case of disaster and in case of contract termination			
98.10	Feasibility to audit/review IT controls of the third party or obtaining independent review report for the same from CERT-In empaneled security consultant, to ensure it meets Bank's information security requirement.			
98.11	Global security practices			
98.12	Applicable threats, its likelihood and corresponding impact			
	Data segregation, confidentiality, privacy controls at the third party (cloud)			
98.13	Sub-contracting			

Cloud Solution

98	continuous monitoring requirement Exit strategy			
98	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.			
99	Threat Modelling of all activities being performed should be documented and should be shared with the bank on periodic basis			
100	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			
	Architecture			
101	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.			
102	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.			
103	The system must comply with organization's guiding principles & standards for enterprise information security/system architecture			
104	The system must be optimized to minimize their power and memory footprint for better performance			
105	Every design decision of the applications should take into account the optimum use of CPU, memory			
106	System must be designed to be efficient, scalable, manageable, fast, frugal with resources, compos-able and SOA-style self-contained			
107	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			
108	The data architecture must classify data in a number of ways: function, purpose, structure, confidentiality, sensitivity			
109	The solution should have a native support for cloud deployment model			
110	The solution should have detailed, periodically updated data dictionary			
111	Infrastructure diagrams, Security & network architecture, data flow diagrams, documentation and configurations must be up to date, controlled and available to assist in issue resolution.			
	Platform and Solution			
112	The Bidder shall deploy the solution in dedicated cloud instance procured in the name of Bank for hosting the application.			
113	An administrator console to the bank to implement/manage/change organization level archival, retention and Backup policies.			
114	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			
	Scalability and Performance			
115	The solution should support dynamic elasticity to cope up with the change in user loads.			
116	The solution should support horizontal and vertical scaling to meet the Bank's future requirement.			
117	Scaling process to be clearly defined by the Bidder and should not involve any code changes.			
118	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.			
119	Ability to scale linearly			
120	Solution should be able to scale to accommodate future usage loads, such as load balancing, clustering, support for additional CPU cores etc.			
121	Solution should meet performance standards regardless of the location within India			
122	Capability to handle sub second response time			
123	Allow for high capacity to carry out transactions during high volume period			
	Security			
124	The solution should comply with the security guidelines & principles of Bank, RBI and GOI			
125	Data should be protected at rest and in motion			
126	Secure mechanisms and protocols must be used for authentication			
127	When the application fails, it should fail to a state that rejects all subsequent security requests			

Cloud Solution

128	Every failure must be handled as per Risk Management Policy			
129	Application must be designed to recover to a known good state after an exception occurs			
130	A global error handler must be designed to catch unhandled exceptions and an appropriate logging and notification strategy must be designed			
131	Client account, transaction data or any sensitive information is encrypted when in transit.			
132	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			
133	Solution should comply with the IT Security Policy, Cyber Security Policy, and IT Policy of the Bank			
134	Encryption to be used for API, data traveling between platform and other interfacing applications. Integrity of data to be maintained at 100% of time.			
135	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.			
136	The solution should be compliant with DC/DR strategy of Bank			
137	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).			
138	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.			
139	The replication between Primary site and secondary site should be possible in both directions.			
140	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.			
Licensing and implementation requirements				
141	The solution can be put to use bank branches/offices/locations			
142	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			
Support and Maintenance				
143	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.			
144	Bidder should fix bugs identified during the period of contract at no additional cost to the Bank.			
145	Bidder should warrant all the software against defects arising out of faulty design, workmanship etc. throughout the contract period.			
146	Bidder should ensure availability of technical expertise and SMEs to extend continuous support to the on-site team.			
147	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.			
148	Bidder should resume operations from an alternate site with minimum downtime whenever required			
149	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.			
150	Bidder should perform system performance monitoring and publish uptime reports at the frequency desired by the Bank.			
151	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.			
152	Audit Trail - All transactions should be securely logged to detect any modifications.			
153	All historical records of deviation along with user audit trail should be logged for future reference.			
154	All overrides for credit approval or rejection should be logged to create audit trail that can be tracked.			
155	History of each parameter change should be logged.			
156	Users should be able to access audit trails of all the transactions, modifications/changes for audit purpose.			
Reporting				

Cloud Solution

	The system should support all the different reporting requirements of the Bank that includes MIS database instance			
157	§ Customizable user specific reports			
	§ Dashboard requirements			
	§ Technical Audit Log trail reports for access control logs			
	§ Reconciliatory reporting where needed			
	§ System health check dashboard for monitoring health of application including security vulnerabilities.			
	Performance Requirements			
158	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.			
	Scalability Requirements			
159	Scaling process to be clearly defined by the Bidder and should not involve any code changes.			
	Compliance with Bank's policies			
160	The solution provider should not store or share any data outside the Bank's infrastructure.			
161	Ownership of data in the cloud - Solution provider and/or 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			
162	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.			
163	Isolation of Banks data from other customers of Solution provider			
164	Ownership of any/all data generated/fed/stored in the system lies with the bank and Solution provider and/or CSP has no rights or licenses or any IPR on the data.			
165	Log retention should adhere to the time frame as per the Bank's log retention policy.			
166	Data needs to be retained for a time frame as per the Bank's data retention policy.			
167	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.			
168	Access to and disclosure of the Banks information assets by the Solution provider -Information should only be used by the Solution provider strictly for the purpose of the contracted service, and in accordance with the terms of pertaining to such use			
169	Secure removal, return, retention and/ or destruction of assets and data belonging to Bank- Upon termination or upon the direction of the bank			
170	Solution provider 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)			
	Hardware			
171	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.			
172	The Bidder shall configure, deploy, support, and manage the set up for the Bank.			
173	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 & Solution provider must ensure that data is removed from all environments of Solution provider			
174	Solution provider should support Backups on immutable storage with ransomware protection.			