बैंक ऑफ महाराष्ट्र
Bank of Maharashtra
भारत सरकार का उद्यम
एक परिवार एक बैंक

CORRIGENDUM

Please refer to RFP 082020 published on **07.09.2020** inviting proposal from eligible bidders for **Supply, Installation & Maintenance of Security Solutions (Data Loss Prevention (DLP), Data Identification & Classification Tool (DICT), Database Activity Monitoring (DAM), Endpoint Encryption (EE) & Patch Management Solution (PMS).** The corrigendum & reply to pre-bid queries are available on Bank’s website https://www.bankofmaharashtra.in in the Tenders Section.

General Manager
Information Technology

13.11.2020

CORRIGENDUM

Please refer to RFP 082020 published on **07.09.2020** inviting bids for **Supply, Installation & Maintenance of Security Solutions (Data Loss Prevention (DLP), Data Identification & Classification Tool (DICT), Database Activity Monitoring (DAM), Endpoint Encryption (EE) & Patch Management Solution (PMS)**.

Due to present situation arising out of outbreak of COVID-19, the bid submission mode has been changed from physical to online mode.

The bid submission will be through E-Procurement Technologies Ltd. (URL - https://eauction.auctiontiger.net/EPROC/). Bidder manual is also available on the same site.

Bidder has to purchase the tender copy at the cost of Rs.29,500 (Rs.25,000/- + Rs. 4,500/- (GST)) through online mode only (NEFT/RTGS) and upload payment details while submitting the bids online. In case, if the Bidder is an MSME registered vendor and opting for exemption from tender copy cost, they have to upload the MSME registration certificate along with supporting documents in place of payment details.

Bank Account details are as below:

Bank Account No. – 60058099506

Account Name - BANK OF MAHARASHTRA I.T.PAYMENTS

Bank IFSC Code – MAHB0001150

Branch name – Pune Main Branch

Branch Code – 1150

Branch address - Shivaji Nagar Pune

The contact details for any queries related to Profile approval/ Tender information/ online bid submission are as under:

Contact Numbers: +91-9081000427, 9904407997 (Prefer these due to Work from Home)

Sr. No.	**Name**	**Contact Number**	**E-mail ID**
1	Imtiyaz Tajani	079 – 6813 6831	imtiyaz@eptl.in
2	Ekta Maharaj	079 – 6813 6852	ekta.m@eptl.in
3	Nandan Valera	9081000427	nandan.v@eptl.in
4	Fahad Khan	9904406300	Fahad@eptl.in
5	Devendra Rajpurohit	9374519729	devendra.r@eptl.in
6	Nikhil Khalas	9173090675	Nikhil@eptl.in
7	Salina Motani	079 – 6813 6843	salina.motani@eptl.in
8	Sujith Nair	079 – 6813 6857	sujith@eptl.in

Sr. No.	Name	Contact Number	E-mail ID
9	Deepak Narekar	079 – 6813 6863	deepak@eptl.in
10	Jainam Belani	079 – 6813 6820	jainam@eptl.in
11	Devang Patel	079 – 6813 6859	devang@eptl.in

Following correction also be read in the tender document.

1. Amendment/Addition in clauses in RFP are enclosed as Annexure-I.

2. The revised commercial bill of material format is attached as Annexure-II.

(V D Kolhatkar)
General Manager
Information Technology

Annexure - I

1. **Page No. 10: Invitation to the Tender :**

Important Information regarding Bid Submission

RFP Term/Clause no. Invitation of the Tender	As per previous Timelines	Revised Timelines
Last Date for Submission of Bid	21.10.2020 up to 14:00 hrs.	04.12.2020 up to 14:00 hrs.
Time and Date for Opening of Technical Bid	21.10.2020 at 16:00 Hrs	04.12.2020 at 16:00 Hrs

Note:- Except above clause, there is no other change in information regarding Bid submission date.

2. **Page No. 126-129 Annexure 5: Eligibility Criteria Compliance:**

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
1	126	A.5 Criteria to be met by the Bidder	The Bidder should be an authorized partner with the highest partnership level of OEM for at least the last 3 years from the date of this RFP. This partnership may be Indian or Global.	The Bidder should be an authorized partner with the highest partnership level of OEM as on date of publishing of this RFP. This partnership may be Indian or Global.
2	128	A.10 Criteria to be met by the Bidder	The Bidder should have the experience of implementing at least 3 out of the 5 solutions in at least one at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India. The credentials provided could be in the same or different Govt. Sector/Scheduled Commercial Bank/PSU's in India. 1. DLP 2. DICT 3. DAM 4. EE 5. PMS	The Bidder should have the experience of implementing at least 3 out of the 5 solutions in at least one at least one Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India. The credentials provided could be in the same or different Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India. 1. DLP 2. DICT 3. DAM 4. EE 5. PMS The solutions deployed may not necessarily have to be the same proposed product.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
			The solutions deployed may not necessarily have to be the same proposed product.	
3	128	B.1 Criteria to be met by the OEM	The proposed DLP application should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	The proposed DLP application should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India.
4	128	B.2 Criteria to be met by the OEM	The proposed DAM application should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	The proposed DAM application should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India.
5	129	B.3 Criteria to be met by the OEM	The proposed DICT solution should be live in at least one BFSI organization in India.	The proposed DICT solution should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India.
6	129	B.4 Criteria to be met by the OEM	The proposed for EE solution should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	The proposed for EE solution should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India.
7	129	B.5 Criteria to be met by the OEM	The proposed PMS solution should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's in India.	The proposed PMS solution should be live in at least one Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India.
8	129	B.7 Criteria to be met by the OEM	The OEM should have been in existence for a minimum period of five years in India as on 31-Mar-2020.	The OEM should have been in existence for a minimum period of One Year in India as on 31-Mar-2020.

3. Page No. 14 & 15 Clause 2.3.1: Project Schedule :

Stage	Activity	# Weeks	Project Duration(in weeks)	Time Period for completion
1	Submission of Detailed Project Plan including integrating all the present security solutions	2	2	2 weeks from issue of Purchase Order
2	Deployment of Resources at Bank's premises for Solution Proposed	4	4	4 Weeks of issuing the Purchase order to SI
3	Pre Implementation Training to bank staff	1	4	4 Weeks of issuing the Purchase order to SI
4	Delivery of related Hardware/Software, licenses and deployment of resources at bank premises	8	8	8 weeks from issue of Purchase Order
5	Installation and Configuration of Hardware/Applications in DC & DR	2	10	2 weeks after delivery of components specified in Point# 4
6	Integration of Installed security solution with other applicable deployed solution in Bank Environment	3	13	3 weeks after installation & configuration part
7	UAT (functional testing) of Deployed Security Solutions	2	15	2 weeks from after completion of tasks specified in Point# 6
8	Implementation of complete solution as per RFP scope in all locations. Impact analysis after implementation of the solutions need to be examined. To simplify the analysis, bidder can plan to implement one solution at a time. After successful implementation of one solution, next solution can be implemented.	8	23	8 weeks after successful UAT

Stage	Activity	# Weeks	Project Duration(in weeks)	Time Period for completion
9	Post Implementation Training	1		Within 6 months from the Date of Project Signoff

Pert Chart:

Description	W1	W2	W3	W4	W5	W6	W7	W8	W9	W10	W11	W12	W13	W14	W15	W16	W17	W18	W19	W20	W21	W22	W23
Submission of Detailed Project Plan including integrating all the present security solutions	🟦	🟦																					
Deployment of Resources at Bank's premises for Solution Proposed	🟧	🟧	🟧	🟧																			
Pre Implementation Training to bank staff	🟨	🟨	🟨	🟨																			
Delivery of related Hardware/Software and license and deployment of resources at bank premises	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩															
Installation and Configuration of security Hardware/Applications in DC & DR									⬜	⬜													
Integration of Installed security solution with other applicable deployed solution in Bank Environment											🟦	🟦	🟦										
UAT (functional testing) of Deployed Security Solution														🟧	🟧								
Implementation of complete solution as per RFP scope in all location)																🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

4. Page No: 62 & 63, Clause: 6.2 Technical Evaluation criterion, Sub Clause: Scoring for Past Experience (PE)

Bidder and OEM's should provide details of past experience in implementing security solution scoped under this RFP. Past experiences will be calculated for each solution separately. The score obtained by the bidder shall be considered for evaluation as given in the **Annexure 17: Past Experience**. The bidder should provide the details of all the implementations in banks including details of scope of project, number of branches with breakup of the role and proof of implementation experience.

Sr. No.	Past Experience	Score	Max Score
A	**Implementation of Data Loss Prevention (DLP) Solution**		30
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	30	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's//BFSI's in India	20	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's India	15	
B	**Implementation of Data Identification & Classification Tool (DICT)**		30
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	30	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	20	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's India	15	
C	**Implementation of Database Activity Monitoring(DAM) Solution**		30
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	30	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	20	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	15	
D	**Implementation of Endpoint Encryption**		30
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	30	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	20	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	15	
E	**Implementation of Patch Management Solution**		30
	Implemented or under implementation in 3 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	30	
	Implemented or under implementation in 2 or more Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	20	
	Implemented or under implementation in 1 Govt. Sector/Scheduled Commercial Bank/PSU's/BFSI's in India	15	
Total Max Score →			150

5. Additional Clause: "5.2.44 : Make in India" under 5.2 Terms of Reference ('ToR')

Public Procurement (Preference to Make in India), Order 2017 - Revision, regarding.

Bank will follow the guidelines on Public Procurement (Preference to Make in India), Order 2017 (PPP-MII Order), Order No. P-45021/2/2017-BEII dated 15.06.2017, as amended by Order No. P-45021/2/2017-BE-II dated 28.05.2018 and Order No. P-45021/2/2017-BE-II dated 29.05.2019 and revision issued vide letter No. P-45021/2/2017(BE-II) dated 04.06.2020. The local supplier at the time of submission of bid shall be required to provide a certificate as per Format 6.31 from the statutory auditor or cost auditor of the company (in the case of companies). Certificate from the statutory auditor or cost auditor of the company (in case of companies) or from a practicing cost accountant or practicing chartered accountant (in respect of suppliers other than companies) giving the percentage of local content, on their letterhead with Registration Number with seal to be submitted (As per format specified in Annexure-27)

"Annexure 27: FORMAT FOR LOCAL CONTENT"

CERTIFICATION FOR LOCAL CONTENT

To: Date:

The Deputy General Manager
Information Technology,
Bank of Maharashtra,
Lokmangal, 1501,
Shivajinagar, Pune

Dear Sir,

Ref: Your RFF Ref: RFP 082020 for Supply, Installation and Maintenance of security Solutions (DLP, DICT, DAM, EE & PMS).

Bidder Name:

This is to certify that proposed **<services as per scope of work>** is having the local content of % as defined in the above mentioned RFP and amendment thereto.

This certificate is submitted in reference to the Public Procurement (Preference to Make in India), Order 2017 – Revision vide Order No. P-45021/2/2017-PP (BE-II) dated 04th June, 2020.

Signature of Statutory Auditor/Cost Auditor

Registration Number :

Seal :

Countersigned by the bidder:
Bidder - (Authorized Signatory)"

6. Amendment in clauses in RFP:

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
1	13	2.3 Project Scope in brief Clause E	Bank will provide necessary Hardware/System Infrastructure for UAT/Development/production environment, OS, Storage, Server in VM, Racks, required network components & connectivity. Bank has ORACLE ULA in place, however the bidder may also propose solution that uses different database, price of the same shall be included by the bidder in their commercials as per the format. Bidder must quote the price for the same in their commercials as per the format. The successful bidder shall implement the proposed solutions based on the same and take care of installation, configuration, support and its further maintenance.	Bidder shall provide all necessary Hardware/Software for UAT/Production environment, OS, Database, Storage, Servers, Racks and other components required for the proposed solution. Bank shall provide required network components & connectivity. Bidder shall take care of the installation, configuration, support and its further maintenance in the Bank. Bidder has to quote the price by considering the aspects as specified above.
2	13	2.3 Project Scope in brief Clause F	Bidder must maintain all involved application/database level components required for the proposed solution. In case, if Bidder is supplying the customised OS, then the Bidder has to take care of OS level installation, configuration, support and its further maintenance as well.	RFP Clause is removed.
3	13	2.3 Project Scope in brief Clause G	If Bidder is supplying appliances or any other hardware for specific solution components which cannot be hosted at VM level, Bidder must quote the price for the same under hardware cost in their commercials as per the format.	RFP Clause is removed.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
4	15	2.3.3 Training Sub Clause ii	This faculty should be solution certified up to advance level and should provide courseware with adequate lab facility as well. The training should be provided by the OEM employee and should be of minimum 3 days, 8 hours a day for each solution under this RFP. Training should be provided to number of personnel identified by Bank on functional, operational and reporting aspects of the entire security solution. Pre implementation training must be provided before project implementation and post implementation training must be provided after successful implementation. At the end of training participants shall be given certificate of successful completion by the OEM.	This faculty should be solution certified up to advance level and should provide courseware with adequate lab facility as well. The training should be provided by the OEM Employee/Employee of OEM Authorized Partner and should be of minimum 3 days, 8 hours a day for each solution under this RFP. Training should be provided to 5 number of personnel for each solution identified by Bank on functional, operational and reporting aspects of the entire security solution. Pre implementation training must be provided before project implementation and post implementation training must be provided after successful implementation. At the end of training participants shall be given certificate of successful completion by the OEM.
5	21	4.1.14 Bulletin Point 3	Bidder to specify the need of VM or other hardware for storage or hosting of application in their technical bid	RFP Clause is removed.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
6	22	4.1.21 POC (Proof of Concept):	Technically qualified bidders should conduct POC (Proof of Concept) within 1 week (7 Working days from the date of mail sent to the technically qualified bidders) as per the above mentioned scope of work and as per the technical requirements and technical Specifications on the Bank's Network. Performance and impact analysis will also be tested as a part of POC. After successful completion of the POC (Proof of Concept), the commercial bids will be opened only for the technically qualified bidders. The Bank may reject the technically qualified bidder/s, if the solution provided is not technically feasible and does not meet the scope of work, technical requirements & technical specifications during the POC (Proof of Concept). Bank will decide the duration of POC depends upon the count of technically qualified bidders and the proposed OEMs.	Technically qualified bidders should initiate POC (Proof of Concept) within 1 week (7 Working days from the date of mail sent to the technically qualified bidders) as per the above mentioned scope of work and as per the technical requirements and technical Specifications on the Bank's Network. Performance and impact analysis will also be tested as a part of POC. After successful completion of the POC (Proof of Concept), the commercial bids will be opened only for the technically qualified bidders. The Bank may reject the technically qualified bidder/s, if the solution provided is not technically feasible and does not meet the scope of work, technical requirements & technical specifications during the POC (Proof of Concept). Bank will decide the duration of POC depends upon the count of technically qualified bidders and the proposed OEMs.
7	24	Data Loss Prevention (DLP) / Clause 4.2.5 Point (K)	Forensic Capability of searching through all the past traffic	Forensic Capability of searching through all the past Incidents.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
8	25	4.2.13	The Bidder shall provide the training of the deployed solution to the Bank personnel for 1 batch with 8 persons.	RFP Clause is removed.
9	25	Data Loss Prevention (DLP) / Clause 4.2.10	The Bidder shall configure integrity monitoring for the files and ensure write protection wherever necessary	RFP Clause is removed as it is not a DLP functionality.
10	26	4.3.7	Solution should provide a breadth of tools that enable customers to detect sensitive data with Regex, Smart Regex, Categorization using Machine Learning (ML) and natural language processing capabilities do detect PCI, PII, etc., The solution should also be configured to detect specific keywords that may be critical for the Bank.	Solution should provide a breadth of tools that enable customers to detect sensitive data with Regex, Smart Regex, Categorization using Machine Learning (ML)/AI based and natural language processing capabilities do detect PCI, PII, etc., The solution should also be configured to detect specific keywords that may be critical for the Bank.
11	29	4.4.7, Point# 36	The Bidder shall provide the training of the deployed solution to the Bank personnel for 1 batch with 5 personnel.	RFP Clause is removed.
12	29	4.5.10	The Bidder shall provide the administrative training of the deployed solution to the Bank personnel for 1 batch with 5 persons	RFP Clause is removed.
13	31	4.6 Patch Management Solution (PMS)	A single management server shall support up to 2,50,000 endpoints, shortening times for patches with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks.	A single management server shall support up to 30,000 endpoints, shortening times for patches with no loss of endpoint functionality, even over low-bandwidth or globally distributed networks.
14	32	4.6.6	The Bidder shall provide the training of the deployed solution to the Bank personnel for 1 batch with 5 personnel in each batch.	RFP Clause is removed.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
15	38	5.1.4 .1	If the contract is awarded, the Bidder shall furnish a Performance Guarantee to the extent of 15% of the value of the contract within 10 days of signing of the contract. The performance guarantee needs to be for the complete period of the contract and would need to be renewed till the expiry or termination of the contract. If the Performance guarantee is not submitted within 10 days, the Bank reserves the right to cancel the contract. The Performance Guarantee would be returned to the Bidder after the expiry or termination of the contract.	If the contract is awarded, the Bidder shall furnish a Performance Guarantee to the extent of 10% of the value of the contract within 10 days of signing of the contract. The performance guarantee needs to be for the complete period of the contract and would need to be renewed till the expiry or termination of the contract. If the Performance guarantee is not submitted within 10 days, the Bank reserves the right to cancel the contract. The Performance Guarantee would be returned to the Bidder after the expiry or termination of the contract.
16	44	5.2.2 Ownership, Grant and Delivery	The Bidder shall procure and provide a non-exclusive, non-transferable, perpetual license for all the software to be provided as a part of this project. All the licenses shall be purchased in the name of the Bank. The use of software by Bidders on behalf of the Bank would be considered as use thereof by the Bank and the software shall be assignable / transferable to any successor entity of the Bank.	The Bidder shall procure and provide a non-exclusive, non-transferable, subscription based licenses for all the software to be provided as a part of this project. All the licenses shall be purchased in the name of the Bank. The use of software by Bidders on behalf of the Bank would be considered as use thereof by the Bank and the software shall be assignable / transferable to any successor entity of the Bank.
17	69	Performance Measurement:	Security solution shall be generating Alert within 15 minutes from occurrence of event. Solution shall be logging ticket for each alert generated within 5 minutes from alert notification.	Security solutions shall be generating incidents/alerts within 15 minutes from occurrence of event.
18	79	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 4	Proposed solution should also monitor data downloads	RFP Clause is removed as it is not a DLP functionality.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
19	79	1	Proposed solution should have a comprehensive list of pre-defined policies and templates withover 1700+ patterns to identify and classify information pertaining to the Banking and Financial Institutions & in-line with the IT Act of India.	Proposed solution should have a comprehensive list of pre-defined policies and templates with patterns to identify and classify information pertaining to the Banking and Financial Institutions & in-line with the IT Act of India.
20	81	18	The solution should have more than 60 pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application.	The solution should have multiple pre-defined applications and multiple application groups and allow each application/application group to monitor operations like Cut/Copy, Paste, File Access and Screen Capture or Download. Also solution should have the capability to define the third party application.
21	83	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 38	Proposed solution should be able to Configure and distribute action rules, including email notification, blocking, quarantining, redirection, and bouncing.	Proposed solution should be able to Configure and distribute action rules, including email notification, blocking and quarantining
22	85	52	Emails violating DLP policies should be quarantined with an automated email based workflow to remediates to take a single click actions like release or block without having to log into the DLP console	Emails violating DLP policies should be quarantined with an automated email based workflow to remediates to take a single click actions like release or block with/without having to log into the DLP console. Bidder needs to provide a solution which allows policy owners or their reporting manager to release/block the violated emails at DLP (Host or Network or any other means) level only.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
23	86	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 60	Proposed solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network by using Python, complex logic, rating and algorithm can be developed as a custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to the Bank.	Proposed solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network by custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to the Bank.
24	86	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 61	Proposed solution should have highly scalable architecture with centralized management that integrates with data loss prevention, Encryption and Identity Services.	Proposed solution should have highly scalable architecture with centralized management that integrates with data loss prevention for all the egress channels like endpoint,email or web channel
25	86	60	Proposed solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network by using Python, complex logic, rating and algorithm can be developed as a custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to the Bank.	Proposed solution should enforce fingerprinting policy on both network and endpoint channel, even when the endpoint is off network by custom data classifier where customer can use in compound with any existing data classifier to identify sensitive data which is unique to the Bank.
26	86	67	Proposed solution should provide directory based policies to selectively monitor downloads based on user, business units, or directory groups, specific groups of computers and specific groups of users.	Proposed solution should provide directory based policies to selectively monitor web uploads based on user, business units, or directory groups, specific groups of computers and specific groups of users.
27	86	68	Proposed DICT solution should provide for automatic tagging and watermarking all unstructured data, including emails, documents, and images according to Bank‘s policy.	RFP Clause is added as a part of DICT solution technical requirement.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
28	87	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 73	A fully functional and dedicated agent management console should be provided for the Endpoint administrator which should provide for agent troubleshooting and diagnostic tools designed for nonIT users	A fully functional and dedicated agent management console should be provided for the Endpoint administrator which should provide the endpoint status and complete visibility.
29	87	71	Proposed solution should provide pre-defined policies for identifying possible for identifying possible expression that are indicative of cyber bullying , self-destructive pattern or employee discontent , Mail to Self etc.,	Proposed solution should be able to provide pre-defined policies for identifying data sent during unusual hours which contains corporate confidential content related to likes of employee discontent, mail to self etc., For Example: An employee sending office files or confidential information in header/footer during unusual business hours, sharing data as an attachment or email body to personal email IDs.
30	88	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 87	Agent should provide for Centrally enable/disable the SPDY protocol on Internet Explorer and Firefox browsers	RFP Clause is removed as it is not a DLP functionality.
31	88	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 86	Agent should not appear in —Add/Remove Programs and System Tray, and obfuscated in Services and Task Manager	Agent should not appear in —System Tray, and obfuscated in Services and Task Manager. Agent or its service/associated service components cannot be removed by anyone from the endpoint except DLP administrator. Solution must offer clean removal of agent mechanism in case if agent components are corrupted and not removable by DLP administrator.
32	88	87	Agent should provide for Centrally enable/disable the SPDY protocol on Internet Explorer and Firefox browsers	RFP Clause is removed as it is not a DLP functionality.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
33	89	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 104	Proposed Solution should provide for management of agent restart/shutdown, agent enable/disable, log retrieval, setting of logging levels, alerts, and configuration through central console.	Proposed Solution should provide for management of agent visibility and also provide the complete endpoint status. If require the logs can be fetched from the specific Endpoint. Bidder may also propose solution that can allow agent control through central console.
34	89	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 97	Solution should have the capability to enable Bank to set caps on % of CPU and disk, and amount of bandwidth used by agent for minimal impact on endpoint and network	Solution should have the capability to reduce over all system resource consumption by agent based on the synctime and the policies logic.
35	90	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 118	Proposed Solution should provide for Option to configure scan timeout by specifying maximum overall duration or maximum idle period.	Proposed Solution should provide for Option to configure scan frequency and scan time.
36	91	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 130	Proposed Solution Should be able to capture all the data flowing outside of the network even if there is no policy configured to match the data. This data should be used later to do a search for after the fact incident so the admin can do a forensic investigation.	Proposed Solution Should be able to capture all the data flowing outside based on the policies of the network . This data should be used later to do a search for after the fact incident so the administrator can do a forensic investigation.
37	92	141	Proposed Solution should be able to detect and protect for the low volume data leaks over the Network and should able to cumulate the transactions up to 7 days.	Proposed Solution should be able to detect and protect for the low volume data leaks over the Network
38	92	133	Proposed Solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.	Proposed Solution should be able to identify senstive data pattern generated by malware infected PC in order to prevent future data leakage

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
39	93	147	Proposed Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and automatically learn false positives. The solution should enforce policies to detect low and slow data leaks	Proposed Solution should have advanced Machine Learning – Ability to automatically learn sensitive information from copies of information that needs to be protected and automatically learn false positives.
40	93	146	The solution should have ability to detect cumulative malware information leaks. The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns.	The solution should able to detect the data leaks over to competitors and the data sent and uploaded after the office hours predefined patterns.
41	93	152	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.	Proposed solution should have capability to receive mails from email server /email gateway and inspect the content before delivering mails to next hop and should qurantine emails that are in violation of company policy.
42	94	155	The DLP Solution must natively integrate with Cloud based storage solutions like One Drive, Rediff Cloud as well as Box to monitor uploads as well as sharing of data from different assets connected outside the organization. This must be outside endpoint DLP solution.	Proposed Solution must monitor/block sensitive data uploads on cloud based storages.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
43	94	154	The solution should be able to identify data leaked in the form unknown and kwon encrypted format like password protected word document.The solution should be able to identify malicious traffic pattern generated by Malware infected PC in order to prevent future data leakage by the malware.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	The solution should be able to identify data leaked in the form encrypted format like password protected word document. The solution should support quarantine as an action for email policy violations and should allow the policy owner or its reporting manager to review the mail and to release/block the violated emails at DLP (Host or Network or any other means) level only with/without logging into the DLP console.
44	95	165	The proposed 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	The proposed solution should provide Incident Workflow capabilities where policy owner or its reporting manager can remediate the DLP policy violations to release/block the violated emails at DLP (Host or Network or any other means) level only with/without logging into the DLP console.
45	95	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 163	Incident management should the workflow of the selected incident, then select one of the following options Assign,Change Status,Change Severity,Ignore Incident,Tag Incident,Add Comments,Delete,Download Incident,Lock,unlock	Incident management should the workflow of the selected incident, then select one of the following options Assign,Change Status,Change Severity,Ignore Incident,Tag Incident,Add Comments,Delete,Download Incident.
46	96	Technical and Functional Requirements for Data Loss/Leakage Prevention (DLP) Solution /Annexure 1.1/ Point 175	Solution must have the capability for bulk closure of incidents.	Solution must have the capability for bulk operation on incidents.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
47	98	8/1.2	The solution should support the ability to classify on Send, Save/Save As, Print, New Email, Close/Open Document, and other email and document events.	The solution should support the ability to classify on Send, Save/Save As, Print, New Email and other email and document events.
48	98	6/ 1.2	The solution should enable the classification of Word, Excel and PowerPoint documents from within Microsoft Office.	The solution should enable the classiifction of entire office suite from within Microsoft office which includes Word, Excel, Powerpoint, Project and Visio
49	100	33/1.2	The solution should provide the ability to allow user to manually classify file attachment(s) directly within MS Outlook when composing an email without the need to open the attachment and without classifying the original source file.	The solution should provide the ability to ensure that the attachments are classified before attaching and sending the mails.
50	100	29/1.2	The solution should support Machine Learning Categorization to help predict different categories of documents, providing classification suggestion or automation on unknown content in documents and email	The solution should support Machine Learning / AI based Categorization to help predict different categories of documents, providing classification suggestion or automation on unknown content in documents and email
51	100	1.2 Technical and Functional Requirements for Data Identification & Classification Tool (DICT): Point -29	The solution should support Machine Learning Categorization to help predict different categories of documents, providing classification suggestion or automation on unknown content in documents and email	The solution should support Machine Learning / AI Categorization to help predict different categories of documents, providing classification suggestion or automation on unknown content in documents and email. For Example: Solution should support ML/AI to suggest users in classifying a document. This is helpful for the users those who needs assistance in classifying a document.
52	101	1.2 Technical and Functional Requirements for Data Identification & Classification Tool (DICT): Point -34	The solution should support the discovery and identification of large volumes of data, stored both on premise and in the cloud. This includes the scanning of network file shares, SharePoint (on premise and Online), as well as Cloud storage providers.	The solution should support the discovery and identification of large volumes of data, stored both on premise and in the cloud. This includes the scanning of network file shares as well as Cloud based storage.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
53	101	1.2 Technical and Functional Requirements for Data Identification & Classification Tool (DICT): Point -37	The solution should have the ability to scan Windows file shares, SharePoint, SharePoint Online, OneDrive, Dropbox, Box and enforce classification based on content, file attributes, file location	The solution should have the ability to scan Windows file shares as well as cloud based storage and enforce classification based on content, file attributes, file location. Example: One Drive, Google Drive etc.,
54	102	52/1.2	The solution should provide the ability to present the user with a checklist of blocked recipients when a policy violation occurs, and allows the user to manually select the recipients that are allowed to bypass the policy violation. For example, the user can be shown all external recipients and asked to confirm individual recipients before sending the email.	The solution should provide the ability to present the user with a checklist of blocked recipients when a policy violation occurs, and allows the user to manually select the recipients that are allowed to receive the email. For example, the user can be shown all external recipients and asked to confirm individual recipients before sending the email.
55	102	45/1.2	The solution should provide the ability to warn users when opening sensitive Office documents.	The solution should provide visible classification indication in sensitive office documents.
56	102	1.2 Technical and Functional Requirements for Data Identification & Classification Tool (DICT): Point - 46	The solution should provide the ability to prevent printing of sensitive email and Office documents to specific printers.	RFP Clause is added as a part of DLP solution requirement. Clause modified as: The solution should provide the ability to prevent printing of sensitive email and Office documents to printers.
57	104	1.3 Technical and Functional Requirements for Database Monitoring Solution (DAM):Point# 2.2	Windows NT / 2000, 2003, 2008	Windows 2008, 2012, 2016 and above.

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
58	112	10 /Architectue Requirements	The solution must support the following OS: a. Microsoft Windows i. Windows 7 / Windows 8 / Windows 8.1 / Windows 10 (All versions) and latest Endpoint OS released by Microsoft time to time ii Windows 2008 / 2012/ 2016 / 2019 (All Versions) and latest server OS released by Microsoft time to time. b. Macintosh OSX c. UNIX i. Solaris ii. HP-UX iii. IBM AIX d. Linux i. Red Hat (Desktop, Enterprise) ii. Fedora iii. SUSE iv. CentOS v. Ubuntu e. VMWare i. ESXI Server	The solution must support the following OS: a. Microsoft Windows i. Windows 7 / Windows 8 / Windows 8.1 / Windows 10 (All versions) and latest Endpoint OS released by Microsoft time to time ii Windows 2008 / 2012/ 2016 / 2019 (All Versions) and latest server OS released by Microsoft time to time. b. Macintosh OSX c. UNIX i. Solaris ii. HP-UX iii. IBM AIX d. Linux i. Red Hat (Desktop, Enterprise) ii. Fedora iii. SUSE iv. CentOS v. Ubuntu e. VMWare i. ESXI Server. However for OS like Unix /Solaris/HPUX/IBM AIX/VMware ESXI OS which are OEM dependant Patching, The solution should support patch deployment using agentless or Script Based patching and must provide centralized reporting with compliance.
59	112	12 /Architecture Requirements	The solution must support security Patches and Updates for standard Databases including (but not limited to): a. Microsoft SQL server (2000, 2005, 2008, 2012, 2016 and latest SQL versions released by Microsoft time to time) b. Oracle 11g, 12c c. MySql d. DB2	The solution must support security Patches and Updates for standard Databases including (but not limited to): a. Microsoft SQL server (2000, 2005, 2008, 2012, 2016 and latest SQL versions released by Microsoft time to time) b. Oracle 11g, 12c c. MySql d. DB2. However for databases like Oracle ,MySQL ,DB2 which are OEM dependant Patching, The solution should support patch deployment using agentless or Script Based patching and must provide centralized reporting with compliance.
60	115	4/Management of Distribution Points	The Distribution Point should be able to run on other shared computers running non windows platforms like RHEL, SOLARIS,AIX, SUSE, Apple Mac OSX etc.	The Distribution Point should be able to run on other shared computers running platforms like Microsoft / Macintosh /Linux OS platform

Sr	Page No	RFP Term/ Clause No	Clause as per RFP	Clause Revised as
61	116	5/Management of Distribution Points	Ability to On-the-fly move the Distribution Point content cache folder to a different drive having highest space if current drive is out of space.	Ability to On demand Patch Download/On-the-fly move the Distribution Point content cache folder to a different drive having highest space if current drive is out of space.
62	117	1.5 Minimum Technical requirements for Patch Management Solution (PMS):	Solution should provide out-of-box patch assessment without the need to setup/schedule and maintain scan process, if any this assessment should report back near real- time (within minutes) once the agent has downloaded its policies.	Solution must have patch assessment capability.
63	147	Annexure 15: Resource Deployment Plan	L1=4 (Pooled Resources Operates 24x7x365)	L1=5 (Pooled Resources Operates 24x7x365).

General Manager
Information Technology