Bank of Baroda RFP Ref No.BCC:CISO:68:111/227 dated 27/06/2019 **Annexure III**

RESPONSE TO PREBID QUERIES Date : 15 July 2019

S.No.	RFP Page	RFP Point / Section #	Clarification point as stated in the tender document	Comment/ Suggestion/ Deviation/ Query	BOB Clarifications dated 11 Jul 2019
1	12	1.13.7 RFP Validity Period	RFP responses will remain valid and open for evaluation according to their terms for a period of at least six (6) months from the RFP closing date.	Request bank reduce the validity period to a maximum of 90 days from the bid submission date	No change
2	12	1.13.9 Charges Terms and Taxes	By submitting the bid, the Bidder will be deemed to have accepted all the terms and conditions mentioned in the RFP document and the rates quoted by the Bidder will be adequate to complete such work according to the specifications and conditions attached thereto and the Bidder has taken into account all conditions and difficulties that may be encountered during the period of assignment and to have quoted all the commercial rates, which shall include agreed price/ contract amount royalties, transportation, delivery, installation and all other facilities and services necessary for proper completion of the assignment, all taxes inter-alia custom duty, excise duty, VAT, octroi etc except such as may be otherwise provided in the contract document for completion of the assignment.	request bank to confirm the GST which will be applicable as extra on the quoted price.	Please refer to following clause on page no. 59 "*Note:1 All the prices quoted above are inclusive of all taxes, octroi etc except Goods & Services Tax. GST shall be paid by the Bank on actual basis. "* As per above clause, GST shall be paid extra by the Bank at actuals.
3	17	2.3.3.	1. Track file, directory and registry access, movement and shares in real time.	We want to understand the term "movement and shares in real time" in detail, can you please share any such usecase or example with us.	Any unauthorized change or movement of file/directory from one location to another location.
4	17	2.3.3.	2. FIM solution shall provide information such as the chain of events that caused the change, who did the change and when the change was done etc.	Can you please elaborate what does it mean by "chain of event that cause the change"?	Self explanatory
5	17	2.3.3.	4 The FIM solution shall be using wide variety of cryptographic generation algorithms so as to detect evasion through signature weaknesses. The FIM shall be capable of identifying grouping of servers based on service and applying same policy. These servers may have different OS and different applications running on it.	Can you please elaborate in detail what does it mean by "wide variety of cryptographic generation algorithm"?	FIM should be able to use cryptographic generation algorithms to monitor encrypted file to detect any integrity violation.
6	17	2.3.4	Selected Bidder will integrate FIM with QRADAR SIEM tool and also with other security tools, if decided by the Bank.	We request you to share the list of Security Tools other than QRADAR SIEM that are being used at Bank of Baroda	Shall be provided to the successful bidder.

7	18	2.3.9	Configuration of the monitored devices will be out of scope of the vendor. However vendor will have to suggest the detailed commands/guidelines for integration of the in-scope monitored systems and provide onsite assistance while installing the agent in monitored devices. Selected Bidder shall also be responsible to integrate FIM solution with QRADAR SIEM tool, Ticket Management tool or any other monitoring tool.	We would like to understand what other service management tool is being used at Bank of Baroda.	Shall be provided to the successful bidder.
8	19	2.3.11	Bank may at its discretion ask the Bidders to demonstrate (POC) the proposed solution to the Bank. Bank would like the selected Bidder to perform a proof of concept testing in the Bank's environment with DC/DR cutover and meeting the Recovery Point (RPO) and Recovery time objective (RTO) of the proposed solution and demonstrate its integration with the SIEM solution.	How important it is to showcase this feature, since it is a part of deployment stage and not covered in POC.	No change
9	19	2.3.12	The training will be arranged by the vendor/OEM in their premises at the cost of the vendor. All expenses related to training shall be borne by the selected vendor except lodging, boarding and travelling expenses of the Bank staff within India.	We can organize technical training over virtual lab, where all the participants can join and attend the training online.	Noted
10	19	2.4	iii. Integrate FIM with SIEM Solution.	How important it is to showcase this feature, since it is a part of deployment stage and not covered in POC.	No change
11	20	2.5 SERVICE LEVEL AGREEMENT	Service Level Solution Uptime % calculated on monthly basis - Less than 70% Penalty - 100%	Request Bank to CAP maximum penalty under this clause to maximum of 10% of the monthly charges calculated based on FIM running expenditure.	No change
12	20	2.5 SERVICE LEVEL AGREEMENT, 1.a	Service Level Solution Uptime % calculated on monthly basis is 99.5% and above	Since the bank has not asked for HA, request you to consider the Uptime starting from 98% and above.	No change
13	20	2.5	Penalty Penalty as XX% of all inclusive monthly charges calculated based on FIM running expenditure.	Please elaborate on how the monthly charges and service uptime will be calculated.	Please refer to clause 2.5 on page no. 20: 1. *Solution uptime is to be maintained on standalone basis without any consideration of devices in HA mode. If a function is down at the site, the same should be shifted to DR site within the SLA parameters.* *2. FIM running expenditure will include all the AMC/Annual License fees etc.*

14	21	2.7.2, Implementation	Implementation of FIM, configuration and its integration with SIEM should be completed within -6- weeks of issuance of purchase order.	Request bank to modify the calause as "Implementation of FIM, configuration and its integration with SIEM should be completed within -10- weeks of issuance of purchase order"	No change
15	21	2.7.2, Implementation	Device integration shall be carried out in phased manner and all devices shall have to be integrated within 10 weeks of issuance of purchase order.	Request bank to modify the clause as " Device integration shall be carried out in phased manner and all devices shall have to be integrated within 14 weeks of issuance of purchase order. "	No change
16	21	2.7.2	Implementation of FIM, configuration and its integration with SIEM should be completed within -6- weeks of issuance of purchase order	Before starting with 6 week implementation timeline, we would like to generate project baseline and perform discovery worksop including below topics • Defining Scope of baseline • Study Bank security framework • Agree on required baseline for FIM Implementation Are you ok with this?	All prerequisites shall need to be completed within project timelines as defined in clause 2.7.2
17	21	2.8	**Network Architecture** Bank has implemented its DC/DR in Mumbai, Hyderabad and Bangaluru with Link level and device level redundancies. Bank's DC and DR sites are connected to various branches through MPLS link, ISDN links, VSAT. Bank's onsite ATMs are part of the branch network. Offsite ATMs and select remote branches are connected through VSATs. Bank's overseas branches/territories networks are managed by network service providers of international repute.	We would like to understand the Bank of Baroda's Network Architecture in detail especially the Bandwidth availability across multiple geo location.	Shall be discussed with successful bidder.
18	21	2.8	**Details of Information Security Policies** Bank has following Board approved policies: • Information Security Policy • Cyber Security Policy • Business Continuity Plan • Purging and Archival policy • Data Privacy & Protection Policy To complement Information Security Policy, Bank has 22 Standard and Guideline documents covering various aspects of Information Security. In addition, Bank has ISMS framework documents as per ISO27001 standard.	We would like to understand if you would like to monitor compliance against these policies using FIM Solution?	Shall be discussed with successful bidder.

19	26	3.1.12 Payment Terms	FIM Solution supply and Installation. 40% of cost and 100% taxes amount shall be paid against delivery, installation and its integration with SIEM tool and basic User acceptance testing. 30% after completion of Phase I. Balance 30% after completion of Phase II.	Request Bank to revise the clause as below: FIM Solution supply and Installation. 80% of cost and 100% taxes amount shall be paid against delivery, installation and its integration with SIEM tool and basic User acceptance testing. 10% after completion of Phase I. Balance 10% after completion of Phase II.	No change
20	26	3.1.12 Payment Terms	AMC/ARLF/Yearly subscription of updates for Security devices Half yearly basis after expiry of the period.	Request Bank to revise the clause as below: AMC/ARLF/Yearly subscription of updates for Security devices. Half yearly basis after expiry of the period.	No change
21	45	ANNEXURE-E : FIM SOLUTION SPECIFICATIONS, point 1.07, OPERATIONAL REQUIREMENTS	FIM Solution should support file directory recursion.	Request you kindly delete this clause as this specific to one bidder	No change
22	45	ANNEXURE-E : FIM SOLUTION SPECIFICATIONS, point 1.08, OPERATIONAL REQUIREMENTS	FIM Console can view status of machines.	Request you to explain the Status of machines. Also please explain on the use case	No change
23	45	ANNEXURE-E : FIM SOLUTION SPECIFICATIONS, point 1.11, OPERATIONAL REQUIREMENTS	FIM Templates can utilize wildcards or variables (to encompass minor differences in file system contents between systems).	Kindly elaborate the clause and explain the use case	No comment
24	45	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, point 1.16, OPERATIONAL REQUIREMENTS	FIM should have ability to automatically promote baseline.	Kindly explain promoting baseline. Request you to elaborate and clear the use case of the clause	Clause is modified as follows: "FIM should have ability to promote baseline which should be deployed automatically."
25	45	Section IV / Annexure E Point 1.01	FIM Solution should be able to create a single baseline that can be distributed to a group of servers to verify differences from baseline (i.e. configuration verification).	The solution helps in creating baselines for each of the server for changes to be monitored and raises alerts/events for any changes. Please clarify if this is acceptable as the feature.	No change

26	45	Section IV / Annexure E Point 1.02	FIM solution should provide capability for Execution of commands based on integrity violations.	The solution provides alerts based on integrity voilations and can forward to SIEM platform to take actionable decisions. Please clarify if this is acceptable as the feature.	No change
27	45	Section IV / Annexure E Point 1.04	Standard Policy templates should be available in the tool	The solution provides FIM feature by defining monitoring rules that are selected and assigned as per the server role (application and OS platform). The Integrity Monitoring rules describe how server should be scan for and detect changes to a files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. Integrity Monitoring rules can be assigned directly to computers or can be made part of a policy. Please clarify if this meets the bank's requirement.	No change
28	45	Section IV / Annexure E Point 1.05	FIM Solution should have facility to group Files and directories together in policy template (rule blocks).	The solution has the capability to group files and directories by creating monitoring rules, please clarify if this meets the bank's requirement.	No change
29	45	Section IV / Annexure E Point 1.06	FIM Solution should be able to specify severity level to individual files and/or directories.	The solution assigns severity levels in the events generated based on rules created. Please clarify if this meets the bank's requirement.	No change
30	45	Section IV / Annexure E Point 1.07	FIM Solution should support file directory recursion.	Here recursion means monitoring of files and folders and the solution monitors folders / files which are created inside the monitored folder. Please clarify if our understanding is correct.	No change
31	45	Section IV / Annexure E Point 1.14	FIM Solution should be able to monitor snapshot of database from console	FIM rules can be created to monitor the files / registry keys / services created by database if they were modified that could indicate that the software was updated or installed / uninstalled. Please clarify if our understanding is correct.	No change
32	46	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, point 1.17, OPERATIONAL REQUIREMENTS	FIM should be able to auto-promote changes when real-time analysis of change indicates they are inconsequential or beneficial	Request you kindly delete this clause as this specific to one bidder	No change

33	46	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, point 1.28, OPERATIONAL REQUIREMENTS	FIM should enable explanations, descriptions, or labels to be annotated by users.	Kindly explain and elaborate the clause	It is not mandatory however desirable feature.
34	46	Section IV / Annexure E Point 1.18	FIM Management console should be cross platform (i.e. Windows and Unix etc.).	We provide management console which is web-based GUI and can be accessed. Please clarify if our understanding is correct.	Noted
35	46	Section IV / Annexure E Point 1.2	FIM should allow users to quickly compare two versions and quickly isolate changes or differences between versions.	Request you to modify the point as "FIM should allow quickly compare two versions and quickly isolate changes or differences between versions"	No change
36	46	Section IV / Annexure E Point 1.22	FIM should be able to change agent passphrases from console.	Please clarify if passphrase is referenced as a password.	Passphrases are used in place of passwords.
37	46	Section IV / Annexure E Point 1.25	FIM should be able to provide users access from anywhere to a single location which allows them to view, search, and compare configurations.	Please modify as "FIM should be able to access from anywhere to a single location which allows to view, search, and compare configurations".	No change
38	46	Section IV / Annexure E Point 1.27	FIM should be able to arrange and manage monitored components in a number of ways including by location, device type, and responsibility etc	Please clarify if the device type ie referenced to servers to be monitored.	No change
39	46	Section IV / Annexure E Point 1.29	FIM should provide standard sets of defaults and templates for each operating environment	The solution provides FIM feature by using standard monitoring rules provided out-of-box that are selected and assigned as per the server role (application and OS platform). The Integrity Monitoring rules describe how server should be scan for and detect changes to a files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. Integrity Monitoring rules can be assigned directly to computers or can be made part of a policy. Please clarify if this meets the bank's requirement.	No change
40	47	Section IV / Annexure E Point 1.06	FIM should analyze changes in real time to determine if they introduce risk based on conditions under which change was made, type of change made and user-specified severity of a change.	Please clarify the conditions and user-specified severity is referred to the monitored rules and severity set by the FIM administrator.	No change
41	47	Section IV / Annexure E Point 1.09	FIM should be able to verify agent security and pass phrases.	FIM management console provides GUI interface to create / change passwords for the deployed agents. Please clarify if passphrase is referenced as a password.	Passphrases are used in place of passwords.

42	47	Section IV / Annexure E Point 1.00	FIM should provide Interface launch commands (toolbar actions) (GUI Interface) to provide one click actions.	The solution provides alerts and events based on the integrity voilations but doesn't provide the funcionality of blocking the source of changes via one click actions. Instead the triggered alerts or events can be forwarded to a analytics platform to pefrom actionable click actions.	No change
43	47	Section IV / Annexure E Point 1.01	Integration or links to change ticketing systems to correlate and match requested change tickets to actual changes.	The solution includes a REST (Representational State Transfer) Web Services API to allow it's functionality to be integrated with other third-party applications. The API can be leveraged to integrate with existing ticketing system to deliver these capabilities, however we need to test the integration with the mentioned applications that will require involvement of inputs from both sides team to validate the integration scenarios.	No change
44	47	Section IV / Annexure E Point 1.03	FIM should have ability to create tickets and/or incidents in Ticketing system based upon integrity violations.	Our FIM solution includes a REST (Representational State Transfer) Web Services API to allow it's functionality to be integrated with other third-party applications. The API can be leveraged to integrate with existing ticketing system to deliver these capabilities, however we need to test the integration with the mentioned applications that will require involvement of inputs from both sides team to validate the integration scenarios.	No change
45	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, point 1.05, Integration	FIM tool provided by the Bidder should be able to monitor network and security devices.	Request you kindly delete this clause as this specific to one bidder	This clause is not mandatory however good to have.
46	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.00, REPORTING AND ALERTING	FIM should have multiple levels of reporting.	Request you to explain multiple level.	No change
47	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.02, REPORTING AND ALERTING	FIM should be able to send Reports via email.	Do you mean reports generated can be send over email?Kindly clarify	No change

48	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.03, REPORTING AND ALERTING	FIM should provide options to print Reports.	Do you mean reports generated can be printed. Kindly clarify	No change
49	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.06, REPORTING AND ALERTING	Reports can be filtered and searchable.	What levels of filter Bank is looking for. Kindly explain	On all key parameters, reports should be searchable, filterable.
50	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.08, REPORTING AND ALERTING	FIM should provide capabilities to create on demand Reports.	What do you mean on Demand Reports. Please explain	No change
51	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.13, REPORTING AND ALERTING	FIM should specify the relative significance of a change according to the monitoring rules for a system component.	What significance is Bank looking for. Please explain	No change
52	48	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.15, REPORTING AND ALERTING	FIM should allow searching to be predefined or saved for future use by all users.	Kindly elaborate the clause and the use case	No change
53	48	Section IV / Annexure E Point 1.09	FIM reports should be easily customizable	Our FIM solution provides out-of-box ready reporting templates which cannot be customized, although we have API that can be used to provide flexible reporting customization. Please clarify if this meets the bank's requirement.	No change
54	48	Section IV / Annexure E Point 1.11	FIM should alert users when configurations change and introduce risk or non-compliance, and provides details on what change was made and who made the change	Currently we address the feature by generating alerts except for “what change was made” which is currently on our planned roadmap.	No change
55	48	Section IV / Annexure E Point 1.15	FIM should allow searching to be predefined or saved for future use by all users	Currently we provide easy-to-use criteria for searching, hence need not require to save for other users.	No change

56	49	ANNEXURE-E : FIM SOLUTION SPECIFICATION6, Point 1.20, REPORTING AND ALERTING	FIM should have role-based and customizable user interface.	Is the user mentioned is the administrator or local user. Kkndly clarify	FIM should provide Role based access control for different levels of users.
57	49	Section IV / Annexure E Point 1.16	FIM should identify all devices whose configurations differ from their designated baselines, or either contain or are missing specified configuration settings	Please clarify if the devices mentioned are referenced to the servers to be monitored.	No change
58	49	Section IV / Annexure E Point 1.17	FIM should provide Audit logging that provides a change control record for all change activity by recording detected changes, added and deleted devices, modified user accounts, etc.	Our understanding is the "user" term mentioned here is the administrator managing the FIM solution. Please clarify.	No change
59	49	Section IV / Annexure E Point 1.19	FIM should differentiate authorized vs. unauthorized changes based on change window, who made the change, what the change was, etc.	Currently we address the feature by generating alerts on real-time basis except for “what change was made” which is currently on our planned roadmap.	No change
60	49	Section IV / Annexure E Point 1.01	FIM should be able to compare an asset’s configuration state against a pre-defined policy /baseline to determine whether or not the configuration is compliant and suggest remedial action.	Every server have their own unique parameters to be monitored based on their functionality and role, compairing against a pre-defined policy is considered to be a standard feature of policy compliance tools.	No change
61	49	Section IV / Annexure E Point 1.03	FIM should support pre defined policy templates.	The solution provides FIM feature by defining monitoring rules that are selected and assigned as per the server role (application and OS platform). The Integrity Monitoring rules describe how server should be scan for and detect changes to a files, directories, and registry keys and values, as well as changes in installed software, processes, listening ports, and running services. Integrity Monitoring rules can be assigned directly to computers or can be made part of a policy. Please clarify if this meets the bank's requirement.	No change
62	49	Section IV / Annexure E Point 1.07	FIM should support operational/performance policies out-of-the-box for business-critical applications	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be removed.	No change
63	50	Section IV / Annexure E Point 1.10	FIM should have ability to report compliance status based on platforms/ applications/devices etc	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	No change
64	50	Section IV / Annexure E Point 1.11	FIM should provide out-of-the-box remediation guidance to help fix non-compliant configurations	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	No change

65	50	Section IV / Annexure E Point 1.12	Ability to systematically waive policy tests to seamlessly integrate into compliance processes and requirements.	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	FIM should have ability to waive rules to test its impact.
66	50	Section IV / Annexure E Point 1.13	Provides proof to management that various departments are in compliance with set security policies.	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	Tool should carry gap analysis for set security rules and provide proof to the management and various departments.
67	50	Section IV / Annexure E Point 1.14	Ability to report “policy scorecards” to summarize the compliance status of a device.	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	FIM should provide gap analysis of the rule compliance and provide the dashboard of the same.
68	50	Section IV / Annexure E Point 1.15	Ability to assign different weights to different tests that comprise a policy scorecard	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	It is not mandatory however desirable feature.
69	50	Section IV / Annexure E Point 1.16	Ability to ignore certain tests for certain periods of time (i.e. support for policy waivers).	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	No change
70	50	Section IV / Annexure E Point 1.17	Fil should have ability to run, assess configurations against multiple policies without requiring a re-scan	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	No change
71	50	Section IV / Annexure E Point 1.18	Ability to report on current policy waivers in effect and their expiration dates.	This is a policy compliance feature which is a different solution altogether and not a part of FIM scope and hence request to be descope the same.	Ability to report on current rule waivers in effect and their expiration dates.
72	58	Annexure M: Part A	3 a. Cost of Licenses for 180 Monitored Devices for DC	Kindly provide break up of 180 devices as of no. of Servers, Operating systems, Active Directories, etc.	Shall be provided to the successful bidder.
73	59	Annexure M: Part A	3 b. Cost of Licenses for 120 Monitored Devices for DR	Kindly provide break up of 120 devices as of no. of Servers, Operating systems, Active Directories, etc.	Shall be provided to the successful bidder.
74	59	Annexure M: Part A	3 c. Incremental cost of FIM Solution license upgrade from 180 devices to 360 devices (cost shall be paid in slabs(blocks) of 20 licenses on pro rata basis) for DC	Kindly provide breakup of 180 devices to 360 devices.	Shall be provided to the successful bidder.
75	59	Annexure M: Part A	3 d. Incremental cost of FIM Solution license upgrade from 120 devices to 240 devices (cost shall be paid in slabs(blocks) of 20 licenses on pro rata basis) for DR	Kindly provide breakup of 180 devices to 360 devices.	Shall be provided to the successful bidder.
76		Additional Queries		Please share the OS and kernel (for Non-windows) wise distribution on which FIM agents will be installed.	Please refer to clause no. 1.21 unser Annexure 'E' on page 41. Detailed list of devices to be monitored shall be shared with the successful bidder.