Clause in RFP

SN	Clause in RFP	Clarifications/ Changes made
1	**1.6 Payment Terms** …… …… **1. Software Licenses Cost** • 30% of the license cost on delivery of Software Licenses plus applicable tax (wherever applicable) at actuals. • 70% of the license cost on sign-off of 5 use-case plus applicable tax (wherever applicable) at actuals. The required documents to be provided along with original invoice: a) Original delivery challans duly stamped and signed by Vendor's representatives and the Bank Official. …… ……	**1.6 Payment Terms** …… …… **1. Software Licenses Cost** • 30% of the license cost on delivery of Software Licenses plus applicable tax (wherever applicable) at actuals. • 70% of the license cost on **UAT** sign-off of 5 use-case plus applicable tax (wherever applicable) at actuals. The required documents to be provided along with original invoice: a) Original delivery challans duly stamped and signed by Vendor's representatives and the Bank Official. …… ……
2	**3. Terms and conditions** …… ……	**3. Terms and conditions** …… …… **3.12 Additional Clause** **Bank will prefer on premise deployment of Solutions. However in case if bidder is proposing cloud based (in part/full) Solution, it should meet all Regulatory and Government guidelines and compliance requirements.**

Addendum to the following Annexures:

1. **Annexure 01 - Table of Contents**
2. **Annexure 11 - Existing Bank's Stack to Enable IA Use Cases**
3. **Annexure 24 - Letter of Undertaking from OEM on Security and compliance**
4. **Additional Clarification to RFP**

All other Terms & Conditions and Scope are same as per our RFP ref no. BCC:IT:PROC:111:53 Dated 5th December 2019 and subsequent addendum for Selection of Service Provider to Design and Implement Intelligent Automation use cases across multiple banking business value chain.

Annexure 01 - Table of Contents

Eligibility cum Technical Bid envelope to contain the following

Section #	Section Heading	Proforma Given
1	Covering letter certifying compliance of Eligibility & Scope of Work for Selection of Service Provider to Design and Implement Intelligent Automation use cases across multiple banking business value chains.	Bidder to provide
2	Credential letters / Supporting documents	Bidder to provide
3	Eligibility criteria compliance with bidder comments	Annexure 02
4	Application Money Transaction Details	Bidder to Provide
5	Bid Security Letter	Annexure 03
6	Bid Security (Earnest Money Deposit) Or Bid Security Form (Earnest Money Deposit in the form of Bank Guarantee)	Bidder to provide Transaction Details Or DD Or Annexure 04
7	Undertaking from the bidder	Annexure 05
8	Conformity Letter	Annexure 07
9	Executive Technical Summary	Bidder to provide
10	Technical Proposal: The technical proposal response based on proposed strategy / methodology / plan along with resource planning and other should be submitted with pages properly numbered, each page signed and stamped.	Bidder to provide
11	Proposed list of Key personnel	Annexure 12
12	List of Assignments	Annexure 16
13	Bill of Material	Annexure 19
14	Copy of the tender document along with annexures and addendum duly sealed and signed on all the pages of the document / digitally signed tender document.	Bidder to provide
15	Masked price bid (Please note that the masked price bid should be exact reflection of the commercial bid except that the masked price bid **should not contain any financial information)**	Annexure 08
16	Integrity Pact (Duly Signed and Stamped by Authorized Signatory on proper stamp paper)	Annexure 21
17	Letter of authorization from the company authorizing the person to sign the tender response and related documents.	**Bidder to provide**
18	A certified copy of the resolution of Board, authenticated by Company Secretary/Director, authorizing an official/s of the company or a Power of Attorney copy to discuss, sign agreements/contracts	**Bidder to provide**

Section #	Section Heading	Proforma Given
	with the Bank.	
19	Undertaking from OEM	Annexure 22
20	Undertaking for Information Security	Annexure 23
21	**Letter of Undertaking from OEM on Security and compliance**	**Annexure 24**

Commercial Bid (Annexure 09) must be sealed and signed by authorized signatory and must be encrypted through E-signer tool available on the portal https://bobtenders.auctiontiger.net.

The Commercial bid submission as part of the RFP response without encryption are liable to be rejected

Authorized Signatory
Name:
Designation:
Bidder's Corporate Name
Address
Email and Phone #
Date:

Annexure 11 – Existing Bank's Stack to Enable IA Use Cases

Vendor is expected to leverage existing Bank's stack. Relevant stack details are as below:

1. Finacle Core Banking Platform v10.2.17
2. IBM Filenet (Case Manager v 5.3.3, ICM v3.06, CPE v 5.5.3, datacap v9.1.6, WAS v9.0.5)
3. Cloudera Hadoop Platform v5.15.2
4. Finstra Fusion Trade Finance System v2.8
5. Loan Origination System Newgen Omniflow 10.3
6. Red Hat BRMS v7.2
7. Oracle Siebel CRM IPv16
8. Cisco Packaged Contact Center Enterprise - v11.5.1 Telephony
9. Verint Intelligent Call Recording Solution - v15.1 Recording
10. Email Management System (Office 365)
11. **Bank's Digital Banking Platforms – Internet Banking, Mobile Banking**
12. **SMS Gateway**
13. **Payment Gateway**
14. **Debit Card Management System**
15. **Base 24 for ATM transaction data**
16. **Financial Risk Management System (FRMS)**
17. **Debit Card Management System**

Annexure 24 – Letter of Undertaking from OEM on Security and compliance

(Applicable only in case of Cloud based solution)

(***This letter should be on the letterhead of the OEM / OSD / Manufacturer duly signed by an authorized signatory***)

To
Chief Technology Officer
Bank of Baroda, Baroda Sun Tower
Bandra Kurla Complex
Bandra (E), Mumbai 400 051

Sir,

We …… (Name of the OEM / OSD) who are established and reputable manufacturers / developers of …… do hereby undertake the following:

1. The proposed solution is complying with the Information security policy of the bank for the applicable solution requirements mentioned in RFP.
2. The solution will be offered at dedicated environment to have better control over Bank's data due to compliance / security related aspects.
3. The solution conforms to the following industry level certifications:
   - ISO 27001:2013
   - ISO 27018
   - SOC 2
   - SSAE/SOC
   - ISO27018
4. We …… (Name of the OEM / OSD) who is responsible for:
   - Data and application privacy and confidentiality
   - System and software access control and administration
   - Custodial responsibilities for data and other information assets
   - Physical Security of the facilities where the Bank's data resides
   - Physical and logical separation from other customers
   - Defining and following Incident response and reporting procedures
   - Complying with the Password Policy of the Bank
   - Complying with the Data Encryption / Protection requirement of the Bank
   - Integration with Single Sign on / Single Sign on Capabilities inbuilt

We hereby attach our response against the various requirement of Bank as follows.

	Subject	**OEM Response**
1.	**Right to Audit:** Service Provider should provide right to audit as similar to what Bank is having with other shared data centers in India. Bank must have "Rights to Audit" the SP's compliance with the	

	agreement including rights of access to the SP's premises where relevant records and Bank's data is being held. It also include audit rights for the Bank or its appointed auditor (nominee) or regulators as an integral clause in the service agreement.	
2.	**Data and Information Security**: SP to ensure following ▪ Data integrity management. ▪ To provide full disclosure regarding security practices and procedures as stated in their SLAs ▪ Specific identification of all controls used during the data lifecycle. ▪ To maintain a fundamental philosophy of knowing where Bank's data (Logical /Physical) ▪ To determine who should access the data, what their rights and privileges are, and under what conditions these access rights are provided and maintain a "Default Deny All" policy ▪ To define and identify the data classification. SP to enforce the Bank's access requirements based on data classification. ▪ To encrypt data at rest and encrypt data in transit. ▪ To share what compartmentalization techniques are employed to isolate Bank data from other customer's data ▪ Sharing of encryption management with Bank on multi-tenant storage. ▪ To comply with data retention and destruction schedules/Policy provided by Bank, SP to certify on Bank's request destroying all data at all locations including slack in data structures and on the media. The Bank will have right to audit this practice. ▪ Understand the logical segregation of information and protective controls implemented. ▪ Understand Cloud provider policies and processes for data retention and destruction and how they compare with internal organizational policy. ▪ Perform regular backup and recovery tests to assure that logical segregation and controls are effective. ▪ Ensure that Cloud provider personnel controls are in place to provide a logical segregation of duties. ▪ To provide Forensic Investigation Support as and when required by the Bank. ▪ To comply with Bank's RTO/RPO requirement and retention policy.	

	▪ In case of cloud based solution the services will be provided only through Data Centers located in India. ▪ In case of cloud based Solution no customer sensitive information or PII information will be saved or transferred to cloud.	
3.	**Application and Process Security:** ▪ SP application should meet the requirements for zoning security, and prevent direct access from the user interface layers to the database layers. The application needs to follow a multi-tier deployment model to achieve this. ▪ The SP application should conforms to Open Web Application Security project guidelines on web application security, including protection against SQL injection, cross-site scripting, data validation for special characters etc. ▪ The application should conform to applicable security guidelines from relevant standards. E.g. ISO/IEC 27017, ISO/IEC 20018. ▪ The application executable files and the source code need to be secured from unauthorized access and possible theft. ▪ If the application is deployed on the Cloud using native multi-tenancy features offered by the application, privacy of data across tenants or entities needs to be ensured through appropriate access control mechanisms ▪ Application should clearly log business errors and technical errors separately to support separation of duties between business users and data Center operator. ▪ User access to sensitive data needs to be controlled ▪ SP to comply with Bank's password management policy. ▪ Features like session timeouts and restricting logins to office hours should be implemented to enhance security ▪ The application should clear sensitive data like passwords from memory immediately after it is processed. ▪ Application level support for definition of users, roles, and exception management functions is to be ensured	
4.	**Integration with external applications**: ▪ Application needs to have well defined APIs and application needs to ensure that only authorized application can invoke such APIs.	

	▪ The application must have extensive audits to log all transactions and important non transactional activities. The application needs to implement maker-checker principle for activities like important business parameter updates. ▪ The application should provide a mechanism to purge old data (after archival if required) while maintaining transactional integrity. ▪ The application should provide a mechanism for Real Time purging while maintaining transactional integrity. ▪ The application needs to provide a documented mechanism, preferably a tool for application monitoring. ▪ The application needs to provide a documented mechanism, preferably a tool for reporting important errors and taking automated actions.	
5.	**IT Infrastructure Security of public cloud consist monitoring as under:** ▪ 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. ▪ 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 in ongoing basis. ▪ Monitoring: Devices should be integrated with SBSOC 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.	
6.	**Physical and Logical Security:** ▪ The SP infrastructure including servers, routers, storage devices, power supplies, and other components that support operations, should be physically secured. Safeguards include the adequate control and monitoring of physical access using biometric access control measures and closed circuit television (CCTV) monitoring. ▪ A security plan for the physical environment should be implemented. Bank should have audit rights on complete physical setup. Data should be	

	have relevant standard certifications and accreditation.	
7.	**Logical Security:** ▪ In a SP environment where business critical data and information systems are coexisting at multiple places, logical security has a very important role in securing the data. To manage logical access Bank should design access using username, password, OTP, RSA Token, Biometric Authentication, etc.	
8.	**Legal Issues:** ▪ There are various laws like Information Technology Act, Data Privacy Act, Data Retention Directive, E-Privacy Directive, E-Commerce Directive, will be applicable to SP providers and also the customers of the Cloud service. Compliance with Indian data privacy law is expected at all times. It will be mandatory to protect the data privacy as per this law. SP should comply with such laws.	
9.	**Operational Security:** ▪ In view of operational security concerns like BCP, DRP, SLA etc., SP need to submit various reports as required by the bank, time to time for internal or regulatory reporting purposes.	
10.	**Miscellaneous:** SP to ensure the following requirements are met ▪ Compliance with Information Security of the Bank as applicable on relevant aspects ▪ Protection mechanism (physical and logical) SP has in place for the actual hardware where Bank's data will be stored on. ▪ Incident management, business continuity and disaster recovery policies, and processes and procedures of service provider (SP) and should include reviews of collocation and back-up facilities.	
11	**Government requests for audits, compliance etc.** In case, if a government demand is received for any data, the below mentioned process has to be followed: ▪ Disclose customer data when legally required and only after attempting to redirect the request to the customer ▪ Resist government demands that are invalid Prior written permission needs to be taken from the bank for all such requests.	

Authorized Signatory
Name:
Designation:
Vendor's Corporate Name

Additional Clarification to RFP

All other Terms & Conditions and Scope are same as per our RFP ref no. BCC:IT:PROC:111:53 Dated 5th December 2019 and subsequent addendum for Selection of Service Provider to Design and Implement Intelligent Automation use cases across multiple banking business value chain.

1. Email Response Management

- **Business Process Details**
  i. Email Response Management process considered by the bank for intelligent automation covers receiving a customer email, categorizing the email into a relevant category, creating a ticket and providing a resolution. For the first six months, it is expected to handle top 10-issues on eight of Bank's service IDs. The details of the use-case are mentioned in annexure 13, the bidders are expected to consider sub-process level details based on their understanding of banking processes.
  ii. The emails are expected to have structured/unstructured data including attachments in emails and screenshots in the email body.
  iii. The emails written in English and Hinglish are a part of scope for the first 6 months.
  iv. The bidders are requested to re-imagine the Email Response Management based on domain knowledge, understanding of regulatory landscape and the best practices for a delightful customer experience.
  v. The bank is expecting "AI at Scale" solution comprising of various relevant AI technologies to support the envisioned journey, bidders are requested to propose the solution accordingly.
  vi. The bidders are requested to make assumptions on any process details which are not explicitly mention in RFP or the subsequent addendums based on their industry experience.
- **Integrations**
  i. Internal and external integrations would be dependent on the envisioned journey. The bidders are expected to consider cost of external integrations or services in the commercials.
- **Business-Case**
  i. The bank expects 50% improvement in business value without impacting the business efficacy. For ex. Reducing cost/ Email Response by 50% without increasing average TAT for resolution of an Email.
  ii. Exact KPIs will be agreed with the relevant business team during the discovery phase of the use-case.

2. Automated Voice Based Interaction on Phone

- **Business Process Details**
  i. Inbound Call Handling considered by the bank for intelligent automation for first 6 months involves responding to customer calls for top 10 customer issues; the bidders are expected to leverage their domain expertise to identify top 10 issues in inbound customer service call center
  ii. Inbound Call Handling considered by the bank for intelligent automation cover:

a) Understand the user request
b) Identify resolution by fetching relevant account or customer level details
c) Communicate resolution to the customers
d) Handover to manual agent in case of a drop-off

iii. The bidders are expected to refer to the annexure 13 for volumetric
iv. The inbound call process is expected to support 3 languages as a part of scope for the first 6 months – English, Hindi and Hinglish
v. The bidders are requested to reimagine the inbound call handling process based on their domain knowledge, understanding of regulatory landscape and the best practices in the domestic and global markets.
vi. The bank is expecting "AI at Scale" solution comprising of various relevant AI technologies to support the envisioned journey, bidders are requested to propose the solution accordingly
vii. The bidders are requested to make assumptions on any process details which are not explicitly mention in RFP or the subsequent addendums based on their industry experience

- **Integrations**

i. Internal and external integrations would be dependent on the envisioned journey. The bidders are expected to consider cost of external integrations or services in the commercials.

- **Business-Case**

i. The bank expects 50% improvement in business value without impacting the business efficacy. For ex. Reducing cost/ call by 50% without increasing average TAT for resolution.
ii. Exact KPIs will be agreed with the relevant business team during the discovery phase of the use-case.

S. No.	Particulars	#
1	Hours of Operations	24/7
2	Working Days	All days
Average matrix in a day		
3	Numbers of Calls	41314
4	Call Completed	39488
5	Call Abandon	1826
6	Average Talk Time (Inbound Calls)	269
8	Average wait time in queue (in sec)	6.44

3. Home Loan Underwriting

- **Business Process Details**

i. Home loan underwriting process considered by the bank for intelligent automation broadly covers submission of application form, collection of documents, data entry into loan origination system and creation of credit sanction note. The bidders are expected to add granularity based on their understanding of banking processes.

ii. The bidders are requested to reimagine the loan application and underwriting process based on their domain knowledge, understanding of regulatory landscape and the best practices in the domestic and global markets.
iii. The bank is expecting "AI at Scale" solution comprising of various relevant AI technologies to support the envisioned journey, bidders are requested to propose the solution accordingly.
iv. The bidders should assume documents supporting these journeys as per laws of the land and typical processes in the banking industry.
v. The bank has FICO's acquisition score-card engine, the bidders are not expected to factor-in any efforts for computation of acquisition scores.
vi. The bidders are requested to make assumptions on any process details which are not explicitly mention in RFP or the subsequent addendums based on their industry experience.

- **Volumetric**
  - The current volumetric are as follows:

Number of Home Loan Applications	12,000 Per Month
% Salaried Customers	40%
Average number of (co-applicant+ guarantors) per application	0.7

  - Request to consider 25% Y-o-Y changes in the application volume.
- **Integrations**
  i. Internal and external integrations would be dependent on the envisioned journey. The bidders are expected to consider cost of external integrations or services in the commercials.
  ii. The bank has a Loan Lifecycle Processing System (LLPS) which acts as a loan origination system. LLPS has integrations available for CIBIL Bureau and NSDL. LLPS will act a downstream system for the envisioned home loan journey. The bank will make LLPS APIs available for integration purpose.

- **Business-Case**
  i. The bank expects 50% improvement in business value without impacting the business efficacy. For ex. Reducing cost/ application by 50% without increasing average TAT for an application.
  ii. Exact KPIs will be agreed with the relevant business team during the discovery phase of the use-case.

4. Outbound Calling and Interaction for Cross-Sell/ Up-Sell, Delinquent Customers, Debit Card Hot Listing

- **Business Process Details**
  i. Outbound Call Handling considered for 6 months by the bank for intelligent automation is for 3 categories – cross sell/upsell, delinquency and emergency (Hot listing, Fraud notification)
  ii. Outbound Call use-cases considered by the bank for intelligent automation cover:

a) Call customer for up-sell/ cross-sell campaigns, provide offer details, answer product/ offer queries, capture customer disposition
b) Call delinquent/ NPA customers for following up on the due payment, provide relevant loan details, capture customer disposition
c) Call customers in case of card hot listing or fraud and guide them towards resolution

iii. The bidders are expected to refer to the annexure 13 for volumetric
iv. The bank has already implemented analytics solutions for identifying cross-sell, up-sell leads, delinquent and NPA customers, hot listing/ fraud cases; the bidders are not expected to factor-in these efforts, customer base for the aforesaid use-cases will be made available at a defined frequency
v. The outbound call process is expected to support 3 languages as a part of scope for the first 6 months – English, Hindi and Hinglish
vi. The bidders are requested to re-imagine the Outbound Call journey based on domain knowledge, understanding of regulatory landscape and the best practices for a delightful customer experience.
vii. The bank is expecting "AI at Scale" solution comprising of various relevant AI technologies to support the envisioned journey, bidders are requested to propose the solution accordingly.
viii. The bidders are requested to make assumptions on any process details which are not explicitly mention in RFP or the subsequent addendums based on their industry experience.

- **Integrations**
  i. Internal and external integrations would be dependent on the envisioned journey. The bidders are expected to consider cost of external integrations or services in the commercials.
- **Business-Case**
  i. The bank expects 50% improvement in business value without impacting the business efficacy. For ex. 50% reduction in cost/ call without reducing the flow backward rate
  ii. Exact KPIs will be agreed with the relevant business team during the discovery phase of the use-case.

5. Trade Finance Digitization & Automation

- **Business Process Details**
  i. Trade finance function considered for 6 months by the bank for intelligent automation is for 3 processes – outward remittances, bill collection and LC issuance
  ii. Intelligent automation broadly covers for following activities across these processes:
    a) Extract data from trade documents. The bidders are expected to assume documents supporting these processes as per laws of the land and typical processes in the banking industry
    b) Classify these documents and enable consistency checks for extracted data across these trade documents, application form and external sources
    c) Manage user workflow for different stakeholders involved in the processes
    d) Auto populate fields for processing applications

e) Auto creation of SWIFT messages and auto interpretation of incoming SWIFT messages

iii. The bidders are requested to reimagine the trade finance processes based on their domain knowledge, understanding of regulatory landscape and the best practices in the domestic and global markets.

iv. The bank is expecting "AI at Scale" solution comprising of various relevant AI technologies to support the envisioned journey, bidders are requested to propose the solution accordingly.

v. The bidders are requested to make assumptions on any process details which are not explicitly mention in RFP or the subsequent addendums based on their industry experience.

- **Integrations**

i. Internal and external integrations would be dependent on the envisioned journey. The bidders are expected to consider cost of external integrations or services in the commercials.

ii. The bank has Misys application (Finstra Fusion Trade) which acts as a trade finance application processing system with in-built workflow management system. Misys will act a downstream system for the envisioned trade finance journeys

iii. Integration with Core Banking System (CBS) for posting of SWIFT messages

iv. The bank will make Misys, CBS APIs available for integration purpose

- **Business-Case**

i. The bank expects 50% improvement in business value without impacting the business efficacy. For ex. reducing cost/ trade finance application by 50% without increasing average TAT for an application.

Exact KPIs will be agreed with the relevant business team during the discovery phase of the use-case