**RFP Ref: SBI/GITC/Platform Engineering-III/2024/2025/1249 dated 03.12.2024**

**Responses to Prebid Queries discussed in the meeting dated 17.12.2024**

| Sl. No | RFP Page No | RFP Clause No. | Existing Clause | Query/Suggestions | Bank's response |
|---|---|---|---|---|---|
| 1 | 3 | Schedule of Events | Last date and time for Bid submission | Request the bank to provide an extension of 4 weeks to complete our internal risk and legal processes and apply to this RFP | Corrigendum issued for extending the Bid Submission date till 03-01-2025 03:00 PM |

| 2 | 10 | 4. SCOPE OF WORK: | As given in Appendix-E of this document.<br><br>Unless otherwise stated under this RFP, all other terms, and conditions of the EOI will be applicable for this RFP. | 1. Can you provide more details on the specific applications and systems that will be integrated into the DevSecOps platform? | Web & Mobile, Monolithic/Service Oriented/Microservice architecture based applications, Internet and Intranet facing applications, 3-tier architecture(App, Web and DB) including legacy applications |
| --- | --- | --- | --- | --- | --- |

| 3 | 10 | 5. ELIGIBILITY AND TECHNICAL CRITERIA | i. Bid is open to all Bidders who meet the eligibility and technical criteria as given in Appendix-B & Appendix-C of this document. The Bidder has to submit the documents substantiating eligibility criteria as mentioned in this RFP document. iii. Skill set and Experience requirements of resources is mentioned in Appendix-P ii. The Bidder shall also submit PRE-CONTRACT INTEGRITY PACT along with technical Bid as prescribed in Appendix-N duly signed by the Bidder on each page and witnessed by two persons. The Pre-Contract Integrity Pact shall be stamped as applicable in the State where it is executed.  Bid submitted without Pre-Contract Integrity Pact, as per the format provided in the RFP, shall not be considered. iii. Skill set and Experience requirements of resources is mentioned in Appendix-P | What are the security protocols and compliance standards that need to be adhered to during the implementation? Please specify, the guidelines provided by the RBI | As per bank's IT/IS Policy/Other related policies/Regulatory requirements |
| 4 | 10 | 5. ELIGIBILITY AND TECHNICAL CRITERIA | The Bidder shall also submit **PRE-CONTRACT INTEGRITY PACT** along with technical Bid as prescribed in **Appendix-N** duly signed by the Bidder on each page and witnessed by two persons. The **Pre-Contract Integrity Pact** shall be stamped as applicable in the State where it is executed.  Bid submitted without Pre-Contract Integrity Pact, | Bidder Seeks Deletion of Clause | The clause cannot be deleted as it is as per bank's requirements. |

| | | | as per the format provided in the RFP, shall not be considered. | | |
|---|---|---|---|---|---|
| 5 | 13 | 8.EARNEST MONEY DEPOSIT (EMD): | ix. If EMD is forfeited for any reasons mentioned above, the concerned Bidder may be debarred from participating in the RFPs floated by the Bank/this department, in future, as per sole discretion of the Bank. | Bidder Seeks Deletion of Clause | The clause cannot be deleted as it is as per bank's requirements. |
| 6 | 27 | 37. LIQUIDATED DAMAGES | A sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 5% of total Project Cost. | Is there an overall cap on the total penalties that can be imposed under this contract ? | As per RFP. |
| 7 | 74 | Appendix–I (Other terms and Penalties) | SLA and penalty regarding resource deployment:<br><br>Rs. 25000/- per resource per missing man-day | | |
| 8 | 27 | 37. LIQUIDATED DAMAGES | If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total | **Proposed** - The proposed penalty of 0.5% per week seems excessive. Such a significant penalty could inadvertently incentivize the Service Provider to prioritize speed over quality, potentially leading to | As per RFP. |

| | | | | Project Cost for delay of each week or part thereof maximum up to 5% of total Project Cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement. | suboptimal outcomes. We believe a more collaborative approach, focused on shared success, would be beneficial for both parties. We propose exploring alternative mechanisms, such as incentive-based structures or performance-linked fees, to incentivize timely and quality delivery. | |
|---|---|---|---|---|---|---|
| 9 | 27 | 37.LIQUIDATED DAMAGES | | If Service Provider fails to deliver and perform any or all the Services within the stipulated time, schedule as specified in this RFP/Agreement, the Bank may, without prejudice to its other remedies under the RFP/Agreement, and unless otherwise extension of time is agreed upon without the application of liquidated damages, deduct from the Project Cost, as liquidated damages a sum equivalent to 0.5% of total Project Cost for delay of each week or part thereof maximum up to 5% of total Project Cost. Once the maximum deduction is reached, the Bank may consider termination of the Agreement. | Bidder requests LD shall be charged on value of delayed portion of scope and not on the project cost | As per RFP. |

| 10 | 36 | Appendix-B (Bidder's Eligibility Criteria) | Client references and contact details (email/ landline/ mobile) of customers for whom the Bidder has executed similar projects in India. (Start and End Date of the Project to be mentioned) in the past (At least 02 client references are required) | Since end to end DevSecOps casestudies are limited in Indian Domestic market, we request Bank to consider following amendment in Client reference requirement in the RFP. | As per RFP. |
|----|----|----|----|----|----|
| 11 | 40 | Appendix-C (Technical – Eligibility Parameter) | Indian/Global distinct clients' assignments handled in implementing centralized End-to-end DevSecOps platform during the last five years (FY2019-2024).<br><br>Please Note:<br>• Supporting documents for above should be Purchase / Work Orders, letters from clients on their letter head, contacts of clients etc.<br>• Only such assignments should be described in above table which are directly related to Scope of Work of this RFP and in implementing centralized DevSecOps platform. | **Proposed**: Our extensive experience in DevSecOps, gained through engagements with global clients, can be substantiated through our auditor's (CA or statutory auditor) declaration that will provide detailed information about the project scope, duration and their outcomes and request Bank to consider the same as valid client reference proof. | |
| 12 | 40 | Appendix-C (Technical – Eligibility Parameter) | The bidder must have minimum 5 references, with at least 2 being in the BFSI industry in the last 2 years. DevSecOps solutions or similar services should have been implemented at the referenced clients | | |

| | | | by the bidder without any sub-contracting. | | |
|---|---|---|---|---|---|
| 13 | 41 | Appendix-C (Technical – Eligibility Parameter) | The bidder must have experience of implementing end to end enterprise wide DevSecOps platform and support mandatorily in banking industry, and at least 2 of the following domains - NonBanking Financial Company (NBFC)/ Payment industries/IT MNCs across the last 5 years (FY 2019 to FY 2024). (Experience within own organisation will not be considered) | | |
| 14 | 43 | Appendix-C (Technical – Eligibility Parameter) Annexure C1 | Among these 5 distinct clients minimum 2 clients should be from Indian Public sector/Private Bank. | As similar scope has been limitedly been implemented in Indian Public sector/Private Bank, we request to relax the criteria to India/ global banks in Annexure C1  Our extensive experience in DevSecOps, gained through engagements with global clients, can be substantiated | As per RFP. |

| | | | | through our auditor's (CA or statutory auditor) declaration that will provide detailed information about the project scope, duration and their outcomes and request Bank to consider the same as valid client reference proof. | |
|---|---|---|---|---|---|
| 15 | 44 | Appendix-C (Technical – Eligibility Parameter) Annexure C2 | Skilled DevSecOps resources currently available (Full time) Certifications: As mentioned in Appendix-P. | Please clarify if the resources actually deployed in the project should be a subset of the resources shared in this list | Yes, skilled DevSecOps resources should be available once PO is issued. |
| 16 | 49 | Appendix-E (Scope of Work and Payment Schedule) | The bidder resources will be required to assess the application landscape and onboard applications onto the DevSecOps pipelines tailored to the requirements.<br><br>It must support a wide range of programming languages and frameworks to accommodate diverse development teams and projects. | The scope in the RFP is very high-level, with no details provided on the applications and technologies used. This makes it difficult for us to assess the resource efforts in terms of count or man-months. We request SBI to clarify the number of applications to be | Please refer pg no. 65 *(points 7 & 8)* of the RFP.<br><br>Web & Mobile, Monolithic/Service Oriented/Microservice architecture based applications, Internet and Intranet facing applications, 3-tier architecture(App, Web and DB) including legacy applications |

| | | | | worked on and specify the technology stack being used, so we can have a clear understanding of the requirements. | |
|---|---|---|---|---|---|
| 17 | 49 | Appendix-E (Scope of Work and Payment Schedule) | NA | 1. DevSecOps Platform Solution – Hosted on-premises but cloud ready (What cloud providers, need to be considered)<br><br>2. What are the key performance indicators (KPIs) for the success of this project? | 1. It will be decided as per bank discretion in the scenario of opting for migration.<br><br>2. The bank seeks to ensure that the applications are onboarded in a timely manner as per plan, training is provided by bidder resources to ensure adoption. KPIs to monitor the same are as per the "Dashboarding and metrics" sub-section, and the benchmark for the same will vary based on application. |
| 18 | 50 | Appendix-E (Scope of Work and Payment Schedule)<br>    1. Project planning:<br>        1.2 Backlog management | 1.2 Backlog management<br>The bidder must ensure that the backlog management tool integrated as part of the DevSecOps solution enables orchestration and maintenance of prioritized list of tasks, features, and enhancements that need to be addressed. | Does SBI want to display all user personalized relevant backlog details on common Kyndryl DevSecOps management portal dashboard? For eg- | No. This will need to be configured for each application, and implementation during development and integration with DevSecOps platform. |

| | | | | tickets assigned to specific user. | |
|---|---|---|---|---|---|
| 19 | 51 | Appendix-E (Scope of Work and Payment Schedule) 1. Project planning: 1.5 Document management | 1.5 Document management The bidder must ensure that the document management tool integrated as part of the DevSecOps solution will enable creation, storage, retrieval, and maintenance of project-related documents. This ensures that all relevant information is organized, accessible, and up to date. | Format of document to be managed by document management tool? | The documentation encompasses artefacts across SDLC, such as solution documents, BRDs, excel files with test cases, test reports etc., and the format varies based on the applications. |
| 20 | 52 | Appendix-E (Scope of Work and Payment Schedule) 2. Code Quality Check 2.1 Unit testing | 2.1 Unit testing The bidder must ensure that the unit testing tool integrated as part of the DevSecOps solution enables testing of individual components or modules of the code to ensure they meet quality gates. Due to the language-specific requirements for Unit Test tooling, the bidder is expected to coordinate with departments and tailor unit testing as per applications to be onboarded. | Will SBI be providing the app specific unit test cases? | In cases where the application department is using the unit testing framework, it needs to be integrated into the setup. In cases where unit testing has not been adopted, the bidder resources will be required to configure the testing framework and provide training on usage of unit testing frameworks. This will help the departments in utilizing the unit testing methodology effectively. |

| 21 | 52 | Appendix-E (Scope of Work and Payment Schedule)<br>   2. Code Quality Check<br>     2.1 Unit testing | Unit testing | Are all 42 applications have unit test suite present? | Availability of test suite depends on application to application, and has varying levels of unit testing maturity |
|----|----|----|----|----|----|
| 22 | 52 | Appendix-E (Scope of Work and Payment Schedule)<br>   2. Code Quality Check<br>     2.2 Automated code review | Automated code review | Is automated code review in place in the current environment?<br>If yes, are stage gates are already defined? | The presence of code quality checks and quality gates varies by applications. We are trying to implement and standardize this at an enterprise level with this project. |
| 23 | 53 | Appendix-E (Scope of Work and Payment Schedule)<br>   2. Code Quality Check<br>     2.2 Automated code review & 2.3 Code Security Testing | Automated code review & Code Security Testing | Please specific various technologies in scope<br>Are there mobile applications in scope too | The technologies in scope vary by application, a list of technologies (non-exhaustive) for year 1 applications are as follows:<br><br>**Front-end**:  Angular, HTML, CSS, Java, Kotlin, Angular, Bootstrap etc.<br><br>**Middlewar**e: Java, Kony, C#, Node.js etc.<br><br>**Backend**: Java, Python, Springboot, C#, .net, Cognos, node.js, VB, etc. |

| | | | | | Yes, mobile applications are in scope

In general we have web & mobile, Monolithic/Service Oriented/Microservice architecture based applications, Internet and Intranet facing applications, 3-tier architecture(App, Web and DB) including legacy applications |
|---|---|---|---|---|---|
| 24 | 53 | Appendix-E (Scope of Work and Payment Schedule)<br> 2. Code Quality Check<br> 2.4 Database Change Control | Database Change Control | Is database change control in place under the current setup?<br>Which Databases are currently being used? | Change control management is in place.

Databases like Oracle, MySQL, MongoDB, PostgreSQL, DB2, MS-SQL, Cloudant etc., |

| 25 | 53 | Appendix-E (Scope of Work and Payment Schedule)<br>  2. Code Quality Check<br>    2.4 Database Change Control | 2.4 Database Change Control<br>The bidder must ensure that the DB change versioning tool integrated as part of the DevSecOps solution manages and tracks changes to the database schema and data. This ensures consistency, traceability, and the ability to rollback changes as and when needed, ensuring quicker fixes in case of defects. | 1. Type of DB scripts/code SBI has? Triggers, stored procedures etc.<br>2. List of DBs available at Bank?<br>3. DB Change Control: DB Change versioning Tool --> Could you provide more details on the database type?<br>4. DB Change Control: With context of "This ensures consistency, traceability, and the ability to rollback changes as and when needed". Rollback would be possible, only if the tools and given Database supports" | The database details depend on applications, and applicability of DB versioning will be provided during onboarding. |
| 26 | 54 | Appendix-E (Scope of Work and Payment Schedule)<br>  3. Testing and verification<br>    3.1 Automation testing | 3.1 Automation testing<br>The bidder must ensure that the automation testing tools integrated as part of the DevSecOps solution facilitate creation and usage of scripts to execute predefined test cases, reducing redundant manual efforts. | Does SBI already has automated tests available to execute? | The coverage of automation depends on the application, there are departments using automated tests via Selenium and appium. |

| 27 | 54 | Appendix-E (Scope of Work and Payment Schedule)<br>   3. Testing and verification<br>     3.1 Automation testing | Automation testing | Are automated test suite present for all 42 applications under scope? | The coverage of automation depends on the application, there are departments using automated tests via Selenium and appium.<br><br>In cases where it is not present, the bidder resources will be required to assist the application departments in designing and implementing the same |
|----|----|----|----|----|----|
| 28 | 54 | Appendix-E (Scope of Work and Payment Schedule)<br>   3. Testing and verification<br>     3.1 Automation testing | Automation testing | Will the scope of PwC be only Automation testing ? Will the functional testing be owned by client ? | Yes, functional testing will be conducted by the application owners and UAT team. The bidder is required to integrate any tooling requested by the applications to facilitate the same. |
| 29 | 54 | Appendix-E (Scope of Work and Payment Schedule)<br>   3. Testing and verification<br>     3.1 Automation testing | Automation testing | Low code drag-and-drop interface to design automation workflows without writing code. Under tools Section, it is mentioned Selenium and Appium. Kindly confirm if a no code tool is preferred or Selenium ? | Currently teams use both UiPath for regression tests, and Selenium/Appium for automated tests. Usage of tooling will vary based on application |

| 30 | 54 | Appendix-E (Scope of Work and Payment Schedule)<br>  3. Testing and verification<br>    3.2 Performance testing | Performance testing | Are Performance testing suite present for all 42 applications under scope? | Performance testing suite availability depends on application to application<br><br>In cases where it is not present, the bidder resources will be required to assist the application departments in designing and implementing the same |
|----|----|----|----|----|----|
| 31 | 54 | Appendix-E (Scope of Work and Payment Schedule)<br>  3. Testing and verification<br>    3.2 Performance testing | Performance testing | If we have the existing script for the targeted 42 application, what tool was used for scripting? Is it a single tool or multiple tools? | Usage of tools varies from application to application. In cases where it is not present, the bidder resources will be required to assist the application departments in designing and implementing the same<br><br>Tooling usage varies by department, commonly used tools are JMeter and LoadRunner |

| 32 | 54 | Appendix-E (Scope of Work and Payment Schedule) 3. Testing and verification 3.2 Performance testing | Performance testing | Do we have a preferred Load simulation tool, either freeware or SaaS-based, for creating test suites | Tooling usage varies by department, commonly used tools are JMeter and LoadRunner |
|---|---|---|---|---|---|
| 33 | 54 | Appendix-E (Scope of Work and Payment Schedule) 3. Testing and verification 3.2 Performance testing | Performance testing | What is the maximum target load (virtual users) expected out of the Platform for performance executions | The target load will keep increasing based on the applications to be onboarded. The max number of concurrent users can be considered as 10,000 in the initial stage (GITC + TSP resources) |
| 34 | 55 | Appendix-E (Scope of Work and Payment Schedule) 3. Testing and verification 3.3 API testing | API testing | Are API test suite present for all 42 applications under scope? | The coverage of API testing depends on the application, there are departments using postman for API testing<br><br>In cases where it is not present, the bidder resources will be required to assist the application departments in designing and implementing the same |

| 35 | 55 | Appendix-E (Scope of Work and Payment Schedule) <br>   3. Testing and verification <br>     3.3 API testing | 3.3 API testing <br> The bidder must ensure that the API testing tools integrated as part of the DevSecOps solution enable validation of the functionality, reliability, and security of application programming interfaces (APIs) to ensure they work as expected. | 1. Is API test automation in scope? <br><br> 2. Application Performance & Load Testing will be done by Testing team. DevSecOps team will help to automate the process? Do you need our testing team involvement? | 1. Yes <br><br> 2. The DevSecOps team will be involved in configuring and automating the process. In cases where the testing practice is not in place, the bidder resources will be required to provide training in leveraging the tool |
|---|---|---|---|---|---|
| 36 | 55 | Appendix-E (Scope of Work and Payment Schedule) <br>   3. Testing and verification <br>     3.4 Device farms | Device farms | Is any device farm currently being used? | Usage of device farms varies by applications, tools such as Browserstack are present. The bidder will be required to onboard applications onto the same and provide training in leveraging the same. |
| 37 | 56 | Appendix-E (Scope of Work and Payment Schedule) <br>   3. Testing and verification <br>     3.5 APK/IPA internal distribution | APK/IPA internal distribution | Which platform is currently being used for APK/IPA internal distribution? What is the no of mobile application under scope? | Firebase is currently being used by select departments for APK distribution |

| 38 | 56 | Appendix-E (Scope of Work and Payment Schedule) <br> 3. Testing and verification <br> 3.6 Test data management | Test data management | Which platform is currently being used for Test data management? | There is no centralized test data management platform in place, it varies based on the application |
|---|---|---|---|---|---|
| 39 | 56 | Appendix-E (Scope of Work and Payment Schedule) <br> 3. Testing and verification <br> 3.6 Test data management | 3.6 Test data management <br> The bidder must ensure that the test data management tool integrated as part of the DevSecOps solution should enable creation, management, and maintenance of test data. This will ensure that testing is conducted under realistic and consistent conditions. | Do generated datasets needs to be integrated with automated tests mentioned in section3.1? | The generated datasets can be used for automated tests, but will not exclusively be used for the same. The generated data can be used for manual tests as well |
| 40 | 57 | Appendix-E (Scope of Work and Payment Schedule) <br> 3. Testing and verification <br> 3.7 Vulnerability assessment and penetration testing | Vulnerability assessment and penetration testing | How many API endpoint, Web URLs are in scope for scanning | This will be shared at time of onboarding. |

| 41 | 53/57 | Appendix-E (Scope of Work and Payment Schedule)<br><br>2.3 Code Security Testing / 3.7 Vulnerability assessment and penetration testing / 3.8 Software composition analysis (SCA) | Dashboarding & ticketing | 1. ITSM integration is it also part of the scope?<br>2. Is the scope enabled SecOps tools for multiple pipelines such as UAT/Prod etc. ?<br>3. Artifact signing and validation is not in scope? Please confirm | The integration of ITSM is in scope, for example it can be done for approval of change requests.<br><br>Yes, the scope is enabled for multiple environment pipelines<br><br>Artifact signing and validation is in-scope |
| 42 | 57 | Appendix-E (Scope of Work and Payment Schedule)<br>3. Testing and verification<br>3.8 Software composition analysis (SCA) | 3.8 Software composition analysis (SCA)<br>The bidder must ensure that the SCA tool integrated as part of the DevSecOps solution analyses the application's dependencies and third-party libraries to identify known vulnerabilities, icensing issues, and compliance risks. | Bidders DevSecOps mgmt portal can show the data from jFrog Xray, Blackduck and Gitlab security feature to visualize the security posture of app for consumption. - suggestion | The bidder can configure the visualizations as discussed.<br>In addition, the bidder will be required to incorporate the metrics from the "Dashboarding & metrics" section. The finalized dashboards will be as per discussion between bidder and bank |

| 43 | 58 | Appendix-E *(Scope of Work and Payment Schedule)* <br>   4. Packaging and releasing of developed components <br>     4.2 Cluster build update | 4.2 Cluster build update <br> The bidder must ensure that the cluster build update tool integrated as part of the DevSecOps solution enables update of build and configurations for clustered environments, ensuring that the software can be deployed and managed across multiple nodes or instances. | 1. Is helm chart creation, onboarding, and execution part of scope? <br> 2. Where are secrets managed or planned to be managed? <br> 3. Cluster build update: What kind of cluster is referenced here? | 1. Helm chart creation, onboarding and execution will be application to selective containerized applications <br><br> 2. Secret management practices vary based on application <br><br> 3. This is to use tools such as helm charts to manage and orchestrate kubernetes cluster deployments |
|---|---|---|---|---|---|
| 44 | 59 | Appendix-E (Scope of Work and Payment Schedule) <br>   4. Packaging and releasing of developed components <br>     4.3 Container platform stack | 4.3 Container platform stack <br><br> The bidder must ensure that the container platform stack integrated as part of the DevSecOps solution enables creation and management of containerized environments for deploying and running applications, ensuring consistency and scalability across different environments. | Is OCP/K8 build and support in scope or only integration with DevSecOps? Which tool is finalized? | OCP/K8 is present in selective applications. Build and support of OCP/K8 is in-scope based on application use-case |

| 45 | 59 | Appendix-E (Scope of Work and Payment Schedule) 4. Packaging and releasing of developed components 4.3 Container platform stack | Container platform stack | What is the no of applications running as containerized workload out of these 42 applications? | Containerization adoption varies based on application. In the first year applications (14), less than 30% of applications are leveraging containerized applications |
|---|---|---|---|---|---|
| 46 | 59 | Appendix-E (Scope of Work and Payment Schedule) 4. Packaging and releasing of developed components 4.4 Artifactory (Repository Management) | Artifactory (Repository Management) | Which Artifactory is being used now? | Usage of artifactory varies based on application, a few examples of tools in-use are JFrog Artifactory and Nexus |
| 47 | 60 | Appendix-E (Scope of Work and Payment Schedule) 5. Configuration | Configuration | Which configuration management tool is being used now? | Configuration management tool adoption varies based on application. Deployments are manual, or can use tools such as Ansible |

| 48 | 60 | Appendix-E (Scope of Work and Payment Schedule)<br>   5. Configuration | 5. Configuration<br>The DevSecOps solution setup by the bidder must enable the handling of configuration changes to maintain the integrity and traceability of the software and environment throughout the SDLC. This includes defining, storing, and managing configurations for servers, applications, network devices, and other components. | 1. List of components for which configuration needs to be written, deployed and managed. Bidder recommends Ansible for configuration management.<br>2. Is deployment of configuration management tool in scope? | 1. Ansible can be used for configuration management, and can be finalized based on agreement with the bank<br><br>2. Deployment of configuration management tool is in-scope, and must facilitate use cases such as drift monitoring and management |
| --- | --- | --- | --- | --- | --- |
| 49 | 60 | Appendix-E (Scope of Work and Payment Schedule)<br>   6. Monitoring<br>      6.1 Incident management | Incident management | Which Incident management tool is being used now? | BMC Remedy/Helix is currently in use |
| 50 | 61 | Appendix-E (Scope of Work and Payment Schedule)<br>   6. Monitoring<br>      6.4 Log aggregation and management | Log aggregation and management | Is there any regulatory requirement for complete isolation of prod and non-prod environment? | As per bank's IT/IS Policy |

| 51 | 61 | Appendix-E (Scope of Work and Payment Schedule)<br>    6. Monitoring<br>      6.4 Log aggregation and management | 6.4 Log aggregation and management<br>The bidder must ensure that the log aggregation tool integrated as part of the DevSecOps solution enables generation, collection, centralization, indexing and analysis of logs from bank applications to gain insights into application performance and overall security. | Our understanding is that Log Management is not under our scope. Is that Correct? | Log management setup for DevSecOps will be under the scope of the work |
|----|----|----|----|----|----|
| 52 | 63 | Appendix-E (Scope of Work and Payment Schedule) | Dashboarding and metrics<br>The bidder resources will be required to develop detailed dashboards to be leveraged by both bank leadership and application owners. Integrate metrics into workflows to ensure continuous monitoring and reporting. | 1. Suggestion: Bidder DevSecOps mgmt portal can show the data in form of dashbaords for leadership and app owner view as single pane of glass. Bibber will explore and identify if all metrices are availble through APIs.<br>2. Is it required to do a custom development of Dashboards, or introduce the tools, having the feature to measure the given metrics? | 1. Good Suggestion. Dashboard implementation must enable monitoring of critical DevSecOps metrics stated in the metrics section. The mode of representation will be based on the agreement between bank and bidder, and must enable continuous tracking of metrics.<br><br>2. The tools will be containing the metrics, and in case additional measurement tools are required, bidder can inform the bank of the same. Dashboards must be developed to enable monitoring of key metrics |

| 53 | 64 | Appendix-E (Scope of Work and Payment Schedule) | Implementation Framework | This will be managed through Bidder's DevSecOps mgmt portal | As per RFP. |
|---|---|---|---|---|---|
| 54 | 65 | Appendix-E (Scope of Work and Payment Schedule) 8. Indicative list of tools | 8. Indicative list of tools The bank has prepared an indicative list of tools for each sub-stage to help the bank achieve the target state DevSecOps toolchain. The resources provided by the bidder are expected to have specialized expertise in the finalized tools. | 1. Indicative list of tools: There could be additional tools requirement, based on the assessment of application. Is the Bank open to procure the licenses for that?  2. Indicative list of tools: Is the given list of tools final or based on the assessment, we should be able to recommend new tools.  3. Are there any existing tools or systems that need to be integrated with the new DevSecOps platform? | 1. Yes, the bank will consider procurement of licenses based on the requirements. Procurement will be based on discretion of the bank, and bank can request bidder assistance in procurement  2. Bidder can recommend new tools if deemed necessary, so that the bank can ensure comprehensive design of tools  3. Presence of tools depends on application to application, and the integration will need to cater to individual application requirements |

| 55 | 65 | Appendix-E (Scope of Work and Payment Schedule)<br><br>Additional considerations | Additional considerations | There are a list of the tools which are mentioned in the RFP to set up the platform validated by each department. Should we consider these tools as the final ones for creating the DevSecOps platform?<br><br>If additional tools are needed to be brought in based on the answer to the above question, when will it be verified that it matches all the expectations for each area as mentioned in the RFP? | 1. The list of tools mentioned in the RFP are indicative, and subject to change based on discretion of the bank.  In case there are changes required, bidder may suggest the same.<br><br>2. If additional tools are purchased, then the bidder is required to conduct diligence on capabilities. Any additional, or missing capabilities are to be discussed with the bank |

| 56 | 66 | Appendix-E (Scope of Work and Payment Schedule)<br><br>9. Resource requirements | 14 resources required and will be used as per the defined categorization based on project requirements. The bank reserves the right to request additional resources or reduce deployed resources from the bidder as per change in project requirements. Resources engaged needs to meet our specified educational qualification, certification requirements and years of experience. The resources already engaged with other projects may not be preferred to be engaged with the task under this project. The actual number of resources may increase or decrease depending on the actual requirements during the implementation and support phase.<br><br>**i. Total period of engagement – Five Year.** | The scope in the RFP is unclear. However, the requirement of 14 resources is mentioned on a man-month basis. We request the Bank to provide clarification on the basis of the resource count calculation.<br><br>Please refer to the example below: 1 Project Manager is requested for 37 months. However, the scope in the RFP does not clarify the application quantification, so we would like to understand the basis for the requirement of 1 Project Manager for 37 months. Additionally, the overall cost is expected for 5 years.<br><br>We request the Bank to provide complete clarity on the scope, | As per RFP. |

| | | | | including the technology stack and applications to be worked upon and let vendor to estimate resource requirements accurately. Alternatively, we propose that the vendor be allowed to provide skilled resources solely on a Time and Materials (T&M) basis for the entire 5-year period, with complete ownership of the work managed by SBI | |
|---|---|---|---|---|---|
| 57 | 66 | Appendix-E (Scope of Work and Payment Schedule)<br><br>9. Resource requirements | 14 resources required and will be used as per the defined categorization based on project requirements. | 1. Is the State Bank of India **Global IT Center, Navi Mumba**i is the primary location for all these resources?<br><br>2. Will the majority of these resources be required to work from the office, or will remote work be permitted?<br><br>3. Will the resources | 1. Yes<br><br>2. No remote work<br><br>3. As per Bank's requirement<br><br>4. It is on Man-Months basis |

| | | | | need to work night shifts? | |
|---|---|---|---|---|---|
| | | | | 4. What is the specific leave policy for these resources? Are they entitled to sick leave, casual leave, vacation leave, and other types of leave? | |
| 58 | 68 | Appendix-F (Indicative Price Bid) | The bid should be submitted as the total cost of the project i.e., implementation and support of Centralized DevSecOps Platform for the period of 5-years. | To ensure accurate cost estimation, please clarify whether we should provide a detailed "5-year cost breakdown based on the role-wise resource projections in Appendix Q" (or) "if a total cost estimate for all 14 resources over the 5-year period" is sufficient. | As per RFP. |
| 59 | 169 | Appendix-Q (Tentative Resource Requirement Workplan) | Role wise resource split-up given for each financial year. | | |
| 60 | 68 | Appendix-F (Indicative Price Bid) | Indicative commercial bid for Engaging competent for fourteen (14) resources for | It is mentioned in the RFP that the requirement is for 14 resources to be deployed within 7 days of PO. Please clarify if the | The requirement of resource skills has been provided in appendix-M, and the proposed resource count has been specified in Appendix-F. |

| | | | | resource grouping into different skills is at the discretion of the bidder or if there is a required count of resources across different skillsets | Month-wise requirement can be found in Appendix-N |
|---|---|---|---|---|---|
| 61 | 74 | Appendix–I (Other terms and Penalties) | Other terms and Penalties:<br><br>SLA and penalty regarding resource deployment:<br><br>The bidder must ensure that the resources deployed are available for one man-month, i.e., 24 working days for every month. In case of non-adherence, the penalties mentioned below shall be applied<br><br>Sr. No. Service Level category Penalty Calculation<br>1 Onsite Resource deployment Rs. 25000/- per resource     per missing man-day | What is the maximum penalty cap for the given SLA penalty | As per RFP. |
| 62 | 74 | Appendix–I (Other terms and Penalties) | The bidders should deploy 14 resources on-site for implementing and supporting Centralized DevSecOps Platform as per Skill-set and educational/professional criteria of this RFP within 7 days from the date of issuance of PO | Please clarify if the bidder has to share the resource CVs before the deployment and then we will be given grace period to swap out unselected resources or we have to deploy the resources first and | The bidder should share the resources CVs before deployment. |

| | | | | then the interviews shall happen | |
|---|---|---|---|---|---|
| 63 | 75 | Appendix–J (Service Level Agreement) | Service Level Agreement | Given that this is a Time and Material project where the deliverables are owned by the Bank, we'd like to understand the rationale behind imposing SLAs on the Service Provider's resources. Pls remove Appendix J as it is not applicable in this RFP | SLA must to be executed by the Bidder |
| 64 | 78 | Appendix–J (Service Level Agreement) | Parties understand and agree that under this Agreement, the Bank may time to time, based on its actual requirements issue separate Purchase Order(s) to Service Provider for providing resources on T&M basis and there is no minimum or prior commitment for such orders under this Agreement. | Bidder needs clarity if the scope will be T&M or a Fixed basis for 5 years | T&M basis |

| 65 | 80 | Appendix–J (Service Level Agreement)<br>1. DEFINITIONS & INTERPRETATION | 1.1.9 "EOI" shall mean REQUEST FOR EMPANELMENT OF IT COMPANIES FOR PROVIDING NICHE TECHNOLOGY RESOURCES FOR VARIOUS APPLICATIONS AND IT INITIATIVES OF THE BANK SKILL WISE vide RFP No. SBI/GITC/IT-PartnerRelationship/2023/2024/1042 Dated: 22.09.2023 and unless otherwise specifically stated under this Agreement shall also include the Empanelment Agreement executed between the Bank and Service Provider in pursuant to EOI. | Bidder clarifies the term of this RFP to be considered | As per RFP. |
|----|----|----|----|----|----|
| 66 | 83 | Appendix–J (Service Level Agreement)<br>3.4 Payments | 3.4 Payments<br>3.4.2 The Bank may withhold payment of any product/services that it disputes in good faith and may set-off penalty amount or any other amount which Service Provider owes to the Bank against amount payable to Service provider under this Agreement. However, before levying penalty or recovery of any damages, the Bank shall provide a written notice to Service Provider indicating the reasons for such penalty or recovery of damages. Service Provider shall have the liberty to present its case in writing together with documentary evidences, if any, within 21 (twenty one) days.  Penalty or damages, if any, recoverable from | Bidder request there shall not be any withholding of invoices in case of any disputes | As per RFP. |

| | | | | | |
|---|---|---|---|---|---|
| | | | Service Provider shall be recovered by the Bank through a credit note or revised invoices. In case Service Provider fails to issue credit note/ revised invoice, the Bank shall have right to withhold the payment or set-off penal amount from current invoices. | | |

| 67 | 90 | Appendix–J (Service Level Agreement)<br><br>6. GENERAL INDEMNITY | 6.1 Service Provider agrees and hereby keeps the Bank indemnified and hold harmless against all claims, actions, loss, damages,, costs, expenses, charges, including legal expenses (Attorney, Advocates fees included) which the Bank may suffer or incur on account of (i) Services Provider's breach of its warranties, covenants, responsibilities, declarations or obligations; or (ii) breach of confidentiality obligations mentioned in this Agreement; or (iii) any willful misconduct and gross negligent acts on the part of employees, agents, representatives or sub-contractors (if allowed) of Service Provider. Service Provider agrees to make good the loss suffered by the Bank. The Service provider shall indemnify and keep fully and effectively indemnified and hold harmless the Bank against any fine or penalty levied on the Bank for improper payment of tax for the reasons attributable to the Service Provider<br>6.2 Service Provider hereby undertakes the responsibility to take all possible measures, at no additional cost, to avoid or rectify any issues which thereby results in nonperformance of software/ hardware/ deliverables within reasonable time. The Bank shall | **Proposed** - While we appreciate the intent behind the proposed indemnity clause, We believe that an indemnity clause of this nature could have potential legal and commercial implications for both parties. We would be open to exploring alternative risk-sharing mechanisms that are more equitable and aligned with industry standards. We believe that a more balanced approach, considering the specific circumstances of the project, would be mutually beneficial. | As per RFP. |

| | | | report as far as possible all material defects to Service Provider without undue delay. Service Provider also undertakes to co-operate with other service providers thereby ensuring expected performance covered under scope of work. | | |
|---|---|---|---|---|---|

| 68 | 92 | Appendix–J (Service Level Agreement)<br><br>16.TERMINATION | 16.1 The Bank may, without prejudice to any other remedy for breach of Agreement, by written notice of not less than 30 (thirty) days, terminate the Agreement or respective Purchase Order/SOW in whole or in part:<br>(a) If Service Provider fails to deliver any or all the obligations within the time period specified in the Agreement or respective Purchase Order/SOW, or any extension thereof granted by the Bank;<br>(b) If Service Provider fails to perform any other obligation(s) under the Agreement or respective Purchase Order/SOW;<br>(c) Violations of any terms and conditions stipulated in the RFP;<br>(d) On happening of any termination event mentioned herein above in this Agreement. Prior to providing a written notice of termination to Service Provider under above mentioned sub-clause (i) to (iii), the Bank shall provide Service Provider with a written notice of 30 (thirty) days to cure such breach of the Agreement. If the breach continues or remains unrectified after expiry of cure period, the Bank shall have right to initiate action in accordance with above clause.<br>16.2 Notwithstanding anything contrary contained in this | **Proposed**: Both parties understand that unforeseen circumstances may arise, and either party may need to terminate the Agreement under such circumstances.<br><br>EY will include flexible termination provisions in the Agreement, recognizing that unforeseen circumstances may arise and that a collaborative approach to contract termination is beneficial for both parties.<br><br>"In the event of unforeseen circumstances or changes in regulatory requirements that materially impact our ability to provide the agreed-upon services, EY may, in its sole | As per RFP. |

| | | | Agreement, the Bank may cancel the respective Purchase Order/SOW immediately by giving written notice to Service Provider, if Service Provider fails to meet the delivery schedule/timelines as defined in this Agreement and/or respective Purchase Order(s)/SOW.<br><br>16.3 The Bank, by written notice of not less than 90 (ninety) days, may terminate the Agreement, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of the Service Provider under the contract is terminated, and the date upon which such termination becomes effective. In the event of termination of the Agreement for the Bank's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination.<br><br>16.4 In the event the Bank terminates the Agreement or respective Purchase Order/SOW in whole or in part for the breaches attributable to Service Provider, the bank may procure, upon such terms and in such manner, as it deems appropriate, Services similar to those undelivered and subject to clause 20 Service | discretion, terminate the Agreement or specific Services" | |
|---|---|---|---|---|

| | | | Provider shall be liable to the Bank for any increase in costs for such similar Services. However, Service Provider, in case of part termination, shall continue the performance of the Agreement or respective Purchase Order to the extent not terminated. 16.5 The Bank shall have a right to terminate the Agreement or respective Purchase Order/SOW immediately by giving a notice in writing to Service Provider in the following eventualities: (i) If any Receiver/Liquidator is appointed in connection with the business of Service Provider or Service Provider transfers substantial assets in favour of its creditors or any orders / directions are issued by any Authority / Regulator which has the effect of suspension of the business of Service Provider. (ii) If Service Provider applies to the Court or passes a resolution for voluntary winding up of or any other creditor / person files a petition for winding up or dissolution of Service Provider. (iii) If any acts of commission or omission on the part of Service Provider or its agents, employees, sub-contractors or representatives, in the reasonable opinion of the Bank tantamount to fraud or prejudicial to the interest of the Bank or its | | |

| | | | employees. (iv) Any document, information, data or statement submitted by Service Provider in response to RFP, based on which Service Provider was considered eligible or successful, is found to be false, incorrect or misleading. 16.6 In the event of the termination of the Agreement or respective Purchase Order/SOW Service Provider shall be liable and responsible to return to the Bank all records, documents, data and information including Confidential Information pertains to or relating to the Bank in its possession. 16.7 In the event of termination of the Agreement or respective Purchase Order/SOW for material breach, the Bank shall have the right to report such incident in accordance with the mandatory reporting obligations under the applicable law or regulations. 16.8 Upon termination or expiration of this Agreement, all rights and obligations of the Parties hereunder shall cease, except such rights and obligations as may have accrued on the date of termination or expiration; the obligation of indemnity; obligation of payment; confidentiality obligation; Governing Law clause; Dispute resolution | | |
| --- | --- | --- | --- | --- | --- |

| | | | clause; and any right which a Party may have under the applicable Law | | |
|---|---|---|---|---|---|

| 69 | 92 | Appendix–J (Service Level Agreement) 16. TERMINATION | 16. TERMINATION | In any event of termination of this SoW/Agreement Bank shall pay Kyndryl for all the products and Services provided up to the effective date of termination, in addition for products which are in transit or orders already placed with respective OEMs, prepaid expenses (AMC, Subscription, support) or value of unamortized investments made by Kyndryl and any expenses Kyndryl incurs through termination. Non-payment is also a material breach

Bidder clarifies Kyndryl should also have a right to terminate for non payment with 30 days notice to Bank | As per RFP. |

| 70 | 93 | Appendix–J (Service Level Agreement)<br><br>16. TERMINATION | 16. TERMINATION<br><br>16.3 The Bank, by written notice of not less than 90 (ninety) days, may terminate the Agreement, in whole or in part, at any time for its convenience. The notice of termination shall specify that termination is for the Bank's convenience, the extent to which performance of the Service Provider under the contract is terminated, and the date upon which such termination becomes effective. In the event of termination of the Agreement for the Bank's convenience, Service Provider shall be entitled to receive payment for the Services rendered (delivered) up to the effective date of termination. | In any event of termination of this SoW/Agreement Bank shall pay Kyndryl for all the products and Services provided up to the effective date of termination, in addition for products which are in transit or orders already placed with respective OEMs, prepaid expenses (AMC, Subscription, support) or value of unamortized investments made by Kyndryl and any expenses Kyndryl incurs through termination. Non-payment is also a material breach<br><br>Bidder clarifies Kyndryl should also have a right to terminate for non payment with 30 days notice to Bank | As per RFP. |

| 71 | 93 | Appendix–J (Service Level Agreement) 16. TERMINATION | 16. TERMINATION<br><br>16.4 In the event the Bank terminates the Agreement or respective Purchase Order/SOW in whole or in part for the breaches attributable to Service Provider, the bank may procure, upon such terms and in such manner, as it deems appropriate, Services similar to those undelivered and subject to clause 20 Service Provider shall be liable to the Bank for any increase in costs for such similar Services. However, Service Provider, in case of part termination, shall continue the performance of the Agreement or respective Purchase Order to the extent not terminated. | Bidder seeks Relaxation for the said Risk purchase clause | As per RFP. |
|---|---|---|---|---|---|
| 72 | 94 | Appendix–J (Service Level Agreement) 16. TERMINATION | 16. TERMINATION<br><br>16.5 The Bank shall have a right to terminate the Agreement or respective Purchase Order/SOW immediately by giving a notice in writing to Service Provider in the following eventualities: | Bidder seeks to have a 30 days notice period in case of the given termination events, also<br><br>In any event of termination of this SoW/Agreement Bank shall pay Kyndryl for all the products and Services provided up to the effective date of termination, in addition for products which are in transit | As per RFP. |

| | | | | or orders already placed with respective OEMs, prepaid expenses (AMC, Subscription, support) or value of unamortized investments made by Kyndryl and any expenses Kyndryl incurs through termination. Non-payment is also a material breach | |
|---|---|---|---|---|---|
| 73 | 95 | Appendix–J (Service Level Agreement)<br>    22. NOTICES | 22. NOTICES | How will changes in project scope or requirements be managed? | As per RFP. |
| 74 | 96 | Appendix–J (Service Level Agreement)<br><br>    23.GENERAL TERMS & CONDITIONS | 23.4    NON-HIRE AND NON-SOLICITATION:<br>During the term of this Agreement and for a period of one year thereafter, neither party shall (either directly or indirectly through a third party) employ, solicit to employ, cause to be solicited for the purpose of employment or offer employment to any employee(s) of the other party, or aid any third person to do so, without the specific written consent of the other party. However nothing in this clause shall affect the Bank's regular recruitments as per its recruitment policy and not targeted | **Proposed** - Given the competitive nature of the talent market, non-solicitation clauses can limit our ability to attract and retain top talent. We believe that a more flexible approach would be beneficial for both parties. | As per RFP. |

| | | | to the employees of Service provider. | | |
|---|---|---|---|---|---|
| 75 | 99 | Appendix-J (Service Level Agreement) ANNEXURE-A (DELIVERABLES/SCOPE OF WORK) 8. Risk Management | DELIVERABLES/SCOPE OF WORK 8. Risk Management | What are the identified risks for this project, and what mitigation strategies are in place? | As per RFP. |
| 76 | 107 | Appendix-J (Service Level Agreement) ANNEXURE-E (PENALTY FOR NON PERFORMANCE OF SLA) | PENALTY FOR NON PERFORMANCE OF SLA | The penalty clauses mentioned in this annexure are empty, please clarify | As per RFP. |
| 77 | 108 | Appendix-J (Service Level Agreement) ANNEXURE-E (PENALTY FOR NON PERFORMANCE OF SLA) | PENALTY FOR NON PERFORMANCE OF SLA | Bidder seeks clarity on the SLA Penalty metrics/ Mechanism and capping | As per RFP. |

| 78 | 109 | Appendix-J (Service Level Agreement) ANNEXURE-F (Transition & Knowledge Transfer Plan) | 3. General | Bidder clarifies that any Transition services shall be provided upon payment for such services to bidder in advance | As per RFP. |
|---|---|---|---|---|---|
| 79 | 109 | Appendix-F | Indicative Price Bid | What are the expectations for training and knowledge transfer to the bank's internal teams? | The bidder will be required to ensure that the tools integrated as part of the application onboarding can be adopted by the application tech team. This involved setup of tools, configuration, training to facilitate usage of tools, documentation on processes to be followed to ensure tooling usage. The bank reserves the right to request extensive training and knowledge transfer as per project progression, to ensure that the DevSecOps platform can be leveraged by the respective departments |
| 80 | 120 | Appendix-G (Certificate of Local Content) | Certificate of Local Content | How will data security and privacy be managed, especially | As per bank's IT/IS Policy |

| | | | | concerning sensitive banking information? | |
|---|---|---|---|---|---|
| 81 | 125 | ANNEXURE-G (Data Processing Agreement)<br><br>3. PROCESSOR OBLIGATIONS:<br><br>3.8 Audit Rights: | The Processor shall make available to State Bank of India and any supervisory authority or their representatives the information necessary to demonstrate its compliance with this Agreement and allow for and contribute to audits and inspections by allowing State Bank of India, its Client, a supervisory authority or their representatives to conduct an audit or inspection of that part of the Processor's business which is relevant to the Services [on at least an annual basis (or more frequently when mandated by a relevant supervisory authority or to comply with the Data Protection Legislation) and] on reasonable notice, in relation to the Processing of Personal Data by the Processor. | **Proposed** - While we understand the desire for transparency, it's important to balance this with the need to protect sensitive information. We believe that a more balanced approach to information sharing, considering the specific nature of the engagement and the sensitivity of the information, would be mutually beneficial. | Not applicable |

| 82 | 149 | Appendix–N (PRE CONTRACT INTEGRITY PACT)<br><br>   6. Fall Clause | PRE CONTRACT INTEGRITY PACT<br>6. Fall Clause<br>The BIDDER undertakes that it has not supplied/is not supplying similar product/systems or subsystems at a price lower than that offered in the present Bid in respect of any other Ministry/Department of the Government of India or PSU or any other Bank and if it is found at any stage that similar product/systems or sub systems was supplied by the BIDDER to any other Ministry/Department of the Government of India or a PSU or a Bank at a lower price, then that very price, with due allowance for elapsed time, will be applicable to the present case and the difference in the cost would be refunded by the BIDDER to the BUYER, if the contract has already been concluded. | Bidder seeks deletion of the clause | As per RFP. |
| 83 | 151 | Appendix–N (PRE CONTRACT INTEGRITY PACT)<br><br>   7. Independent Monitors | PRE CONTRACT INTEGRITY PACT<br>7. Independent Monitors<br>7.6 The BIDDER(s) accepts that the Monitor has the right to access without restriction to all Project documentation of the BUYER including that provided by the BIDDER. The BIDDER will also grant the Monitor, upon his request and demonstration of a valid interest, unrestricted and unconditional access | Bidder clarifies, is not obligated to share any information relating to Bidder's costs, Bidder proprietary data, confidential information of Bidder's other customers and internal audit reports of the Bidder. | As per RFP. |

| | | | | | |
|---|---|---|---|---|---|
| | | | to his project documentation. The same is applicable to Subcontractors. The Monitor shall be under contractual obligation to treat the information and documents of the BIDDER/Subcontractor(s) with confidentiality. | | |
| 84 | 158 | Appendix-P | Resource profiles | Are there any specific training programs or certifications required for the resources involved in this project? | All qualifications and resource requirements have been mentioned for each profile. These are the minimum qualifications and the bidder can provide profiles with extensive training and experience in DevSecOps implementation |
| 85 | 163 | Appendix-Q (Tentative Resource Requirement Workplan) | Tentative Resource Requirement Workplan<br>The tentative workplan with roles and resource requirement across phases of the project have been listed below. The list displayed below is subject to change at the discretion of the bank based on project requirements and the bidder is expected to accommodate changes in the same. | The price bid and terms are basis the given projection, in case of any changes the prices are also subject to changes | As per RFP |

| 86 | | General Question | | Bidder requests that all Legal, Financial and Penalty related clauses can be mutually agreed upon if contract is awarded to the bidder | As per RFP. |
|---|---|---|---|---|---|
| 87 | | General Question | | Could you provide details of the existing defects, issues and challenges of the current Setup | The bank currently has siloed application development, with each department leveraging their own SDLC process and tooling. This has led to reliance on manual development and testing processes, and lack of standardization in toolchain across the bank. We seek to increase the importance given to tool standardization, automation of processes, and focus on testing and security processes through this project |

| 88 | | General Question | | Kindly provide Technology Stack and details of applications in scope. E.g. Name of the Applications, the number of modules/Repo | The technologies in scope vary by application, a list of technologies (non-exhaustive) for year 1 applications are as follows:<br><br>**Front-end**:  Angular, HTML, CSS, Java, Kotlin, Angular, Bootstrap etc.<br><br>**Middlewar**e: Java, Kony, C#, Node.js etc.<br><br>**Backend**: Java, Python, Springboot, C#, .net, Cognos, node.js, VB, etc.<br><br>In general we have web & mobile, Monolithic/Service Oriented/Microservice architecture based applications, Internet and Intranet facing applications, 3-tier architecture(App, Web and DB) including legacy applications |
|----|--|------------------|--|-------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 89 | | General Question | | What would be  the various environments, the | Dev/SIT/UAT/PRE-PROD/PROD/DR environments. It may |

| | | | | | DevSecOps Tools need to cater, e.g. Dev/ Test/ Prod | vary from application to application. |
|---|---|---|---|---|---|---|
| 90 | NA | General Question | | | 1. What is the tech stack of the 42 applications that are in scope of this engagement? 2. What is the no of non-prod environments present for each application? 3. Any preferred tool for service mesh? 4. Is there a list compliance requirements that needs to be followed for the DevSecOps platform? If yes, please share the details. 5. Is DR applicable for the DevSecOps platform? | 1. The technologies in scope vary by application, a list of technologies (non-exhaustive) for year 1 applications are as follows:

Front-end:  Angular, HTML, CSS, Java, Kotlin, Angular, Bootstrap etc.

Middleware: Java, Kony, C#, Node.js etc.

Backend: Java, Python, Springboot, C#, .net, Cognos, node.js, VB, etc.

In general we have web & mobile, Monolithic/Service Oriented/Microservice architecture based applications, Internet and Intranet facing applications, 3-tier architecture(App, Web and DB) including legacy applications |

| | | | | | 2. Will be shared at the time of DevSecOps platform designing

3. Will be discussed during Pre-Bid meeting

4. Will be shared during setting up of DevSecOps platform

5. Yes applicable |
| --- | --- | --- | --- | --- | --- |

***