Star Union Dai-ichi Life Insurance Company Limited

Request for Proposal (RFP)

For

DEVSECOPS SOLUTION

Issue Date :-16/10/2025

Last Date of Submission of Proposal: -31/10/2025

Tender Sr. No. :- SUDLIFE/CPD/TD/25-26/009

DISCLAIMERS

The information contained in this Request for Proposal (RFP) document or information provided subsequently to applicants whether verbally or in documentary form by or on behalf of SUD Life is provided to the applicants on the terms and conditions set out in this RFP document and all other terms and conditions subject to which such information is provided. This RFP is neither an agreement nor an offer and is only on invitation by SUD life to the interested parties for submission of proposal. The purpose of this RFP is to provide the applicants with information to assist the formulation of their proposals. This RFP does not claim to contain all the information each applicant may require. Each applicant should conduct its own investigations and analysis and should check the accuracy, reliability and completeness of the information in this RFP and where necessary obtain independent advice. SUD Life makes no representation or warranty & shall incur no liability under any law, statute, rules or regulations as to the accuracy, reliability or completeness of this RFP. SUD Life may in its absolute discretion, but without being under any obligation to do so, update, amend or supplement the information in this RFP. SUD Life reserves the right to accept or reject any RFP without assigning any reasons whatsoever.

1. INTRODUCTION

1.1 About

Star Union Dai-ichi Life Insurance Company Ltd. (SUD Life) is a joint venture between SUDL of India & Union SUDL of India, India's leading public sector SUDLs and The Dai-ichi Life Insurance Company, Japan one of the top ten world leaders in insurance which has been incorporated with the primary objective of carrying out life insurance business in India.

Star Union Dai-ichi Life Insurance Co. Ltd. (SUD Life), with the strength of the domestic partners in the Indian Financial Sector coupled with the Dai-ichi Life's strong domain expertise is a strong player in the Indian Life Insurance market.

1.2 Purpose

The purpose of this RFP is to inform potential Bidders of a business opportunity and to solicit proposals for **DEVSECOPS SOLUTION** as currently contemplated by SUD LIFE. Based upon the review and evaluation of proposals offered in response to this RFP, SUD LIFE may at its sole discretion negotiate and enter into contracts with one or more successful Bidders. Notwithstanding any other provision herein, Bidder participation in this process is voluntary and at Bidder's sole discretion. Price will be a consideration but will not be the sole factor in SUD LIFEs decision to award a contractual relationship. The products, volumes and historical numbers that are provided from SUD LIFE during this process are to be used and interpreted solely as a guide and are intended to provide guidance to SUD LIFE's future or projected requirements but are not guarantee, contract or commitment to any current or future volume or orders. No volume commitment should be inferred from this process or from any of the documentation provided by SUD LIFE. SUD LIFE reserves the right to accept or reject any or all bids from a specific or multiple Bidders for any reason at any time. SUD LIFE also reserves the right at its sole discretion to select or reject any or all Bidder(s) in this process and will not be responsible for any direct or indirect costs incurred by the Bidders in this process.

2. Bid Submission

The Bid (attached formats) duly signed, and super scribed "**Bid for DevSecOps Solution"** should be addressed to

Executive Vice President (Finance Controller)
Star Union Dai-ichi Life Insurance Company Limited

Please note that the Technical and **Commercial bid have to submit online through email and commercial should be password protected at procurement@sudlife.in .** The Company is not responsible for non-receipt of bids by the specified date and time due to any reason including holidays. All questions / clarifications, if any, regarding this tender should be communicated **only** via email at procurement@sudlife.in .

Trademark used under licence from respective owners.

Last date for receipt of any query is 24/10/2025. Bids received after the stipulated date/ time or incomplete in any respect are liable to be rejected.

3. Acknowledgement

Please acknowledge receipt of this document by responding via email to procurement@sudlife.in. Please include the contact information for the person who will be directly responsible for completing the RFP.

4. RFP Schedule

We are listing below the various deadlines to be met to ensure participation

1	**Last date for Submission of Process compliance & Techno commercial Compliance statements (Complete RFP Set along with Technical supporting Document)**	**31/10/2025**
2	**Last date for Submission of Quotes (Annexure D and Proposal Form)**	**31/10/2025**

5. Requirement Overview

5.a. Buyer Profile	Star Union Dai-ichi Life Insurance Company Ltd. (SUD LIFE) is a joint venture between SUDL of India & Union SUDL of India, India's leading public sector SUDLs and The Dai-ichi Life Insurance Company, Japan one of the top ten world leaders in insurance which has been incorporated with the primary objective of carrying out life insurance business in India.
5.b. Services up for Quote	DevSecOps Solution
5.c. Scope of Services	The service provider must clearly understand and conform to the following deliverables for the service of: Detailed scope mentioned in 'Annexure A'
5.d. Operating Days & Hours	NA
5.e. Selection Process of vendors	• You need to sign and send your **Process Compliance and Techno-Commercial statement** in response to this RFP **(Annexure B & C)** • You need to submit the **quote** as per the format mentioned in **Annexure D** • Star Union Dai-ichi will evaluate the final quotes of all the vendors & will decide on awarding business based on the

Trademark used under licence from respective owners.

	Comprehensive value proposition of each service provider.
5.f. Award Decision	• **Supplier must submit the quote by the due date to be considered for the contract.** • Star Union Dai-ichi will decide which vendor will be examined for awards. It is important to note that the **supplier of the lowest price does not automatically win the business**. • Star Union Dai-ichi reserves the **right to split the business** amongst vendors depending on the prices achieved through this process. • The contract will be awarded basis the internal criteria set by Star Union Dai-ichi which comprise Technical Evaluation, Commercial Evaluation & any other factors. The supplier selected for award of the contract, on refusal to accept the contract would be debarred from further dealings with Star Union Dai-ichi. **In the event of you being selected by Star Union Dai-ichi and your subsequent default on your quote, you will be required to pay Star Union Dai-ichi an amount equal to the final quote and the next lowest quote on total quantum of purchase** (indemnity clause).
5.g. Service & Penalty	To be mutually discussed before finalizing the rate contract.
5.h. Payment Term	30 days after the submission of invoice

Trademark used under licence from respective owners.

RELATED PARTY TRANSACTION DECLARATION FORM (BY SERVICE PROVIDER)

Service Provider Name:

Registered Address:

Details of Proposed contract to be entered:

Are you a related party or group entity of SUD Life Insurance Co (herein referred to as 'the Company') or any Insurance Intermediary registered with IRDAI (Insurance Regulatory Development Authority of India)?

☐ Yes ☐ No

Declaration by the Service Provider

I/ We hereby confirm that the involvement of any of the above-mentioned people with the Company or with any of its employees/directors will not in any manner unduly benefit us or the employee(s) of the Company and further confirm that no benefit/advantage have been exchanged between the Service Provider and the employees/directors of the Company in respect of the proposed transaction.

I/ We further confirm that the terms and conditions of the proposed contract will be at market rate and on an arm's length basis

I/ we further confirm that in case if we become group entity/ related of the Company or any insurance intermediary registered with IRDAI (Insurance Regulatory Development Authority of India), then we shall inform the Company regarding the same within 7 days from date such arrangements.

Name:

Signature:

Seal of the Service Provider

Date:

(Authorized Representative)

Trademark used under licence from respective owners.

6. Terms of the RFP

6.1 Hold Harmless

In submitting a proposal, Bidder understands that SUD LIFE will determine at its sole discretion which proposal, if any, is accepted. Bidder waives any right to claim damages of any nature whatsoever based on the selection process, final selection, and any communications associated with the selection. SUD LIFE reserves the right to award the Contract to the Bidder(s) whose proposal is deemed to be the most advantageous in meeting the specifications of the RFP.

6.2 Confidentiality Provision

The terms of this RFP, the information provided by SUD LIFE herein and all other information provided by Bidder in connection with the services to be provided by Bidder pursuant to this RFP, are to be treated by Bidder as strictly confidential and proprietary. Such materials are to be used solely for the purpose of responding to this request. Access shall not be granted to third parties except upon prior consent of SUD LIFE and upon the written agreement of the intended recipient to treat the same as confidential. SUD LIFE may request at any time that any of SUD LIFE's material be returned or destroyed. Should Bidder choose not to respond to this RFP, please return all materials and any duplicates thereof.

6.3 Sub-Contracting

The services offered to be undertaken in response to this RFP shall be undertaken to be provided by the Bidder directly employing their employees, and there shall not be any sub- contracting done by the Bidder.

6.4 Acceptance of Proposals

SUD LIFE reserves the right to modify the terms of the RFP at any time at its sole discretion. After the submission of proposals, interviews and negotiations may be conducted with one or more Bidders, but there will be no obligation to receive further information, whether written or oral, from any Bidder or to disclose the nature of any proposal received. This RFP should not be construed as an agreement to purchase products or services. SUD LIFE is not bound to accept the lowest price or any proposal of those submitted. Proposals will be assessed in accordance with the evaluation criteria.

6.5 Liability for Errors

While SUD LIFE has made considerable efforts to ensure an accurate representation of information in this RFP as per its current understanding of the requirements under the various activities in the scope of work, the information contained in this RFP is supplied as a guideline for Bidders. The information is not guaranteed or warranted accurately by SUD LIFE, nor is it necessarily comprehensive or exhaustive. Nothing in this RFP is intended to relieve Bidders from forming their own opinions and conclusions with respect to the matters addressed in this RFP. In the event SUD LIFE finds that the objectives of the intended activities is better achieved by processes/procedures other than those mentioned in this document, SUD LIFE shall have the right

Trademark used under licence from respective owners.

irrespective of the fact whether it has already received proposals from intending bidders or not, to effect such changes and enter into negotiations with one or more Bidders at its sole discretion for such changed/modified processes.

6.6 Acceptance of Terms

All the terms and conditions of this RFP shall be deemed to be accepted by the Bidder and incorporated in its proposal unless specifically notified otherwise.

6.7 Order Cancellation

Star Union Dai-ichi reserves the right to cancel the order in the event of the vendor failing to deliver services specified by Star Union Dai-ichi as per the Service Level Agreements. Star Union Dai-ichi reserves full right and authority to cancel such order and will also be entitled to claim liquidated damages for the same in addition to and without prejudice to all other rights and remedies that may be available to Star Union Dai-ichi. In case of serious discrepancy in services provided, Star Union Dai-ichi may cancel the entire purchase order.

6.8 Force Majeure

The order is subject to Force Majeure at either the buyer or the supplier's end. Any disputes arising out of or under this order shall be subject to the jurisdiction of the courts in Mumbai only. Any event due to any cause beyond the reasonable control of a Party, including, without limitation, unavailability of any communication system, breach or virus in the internet, sabotage, fire, flood, explosion, acts of God, civil commotion, strikes or industrial action of any kind, riots, insurrection, war, acts of government, computer hacking, unauthorized access to computer data and storage devise, computer crashes, breach of security and encryption, etc.

6.9 Inspection and Audit

The vendor should allow Star Union Dai-ichi, its management, auditors, regulators and /or agents the opportunity of inspecting, examining, auditing and /or taking copies of the vendors operations and business recourse which are relevant to this Agreement and/ or for carrying out the activities as /or financial arrangements/ agreements set forth in this Agreement. Star Union Dai-ichi will have the right to do a Security Audit of the vendor's IT infrastructure. The vendor should make necessary changes / upgrades to the IT systems as may be necessary or as required by Star Union Dai-ichi from time to time to ensure data safety.

6.10 Use of Contract Documents and Information

- The Service Provider shall not, without SUD Life's prior written consent, disclose the Contract, or any provision thereof, or any specification, plan, drawing, pattern, sample or information furnished by or on behalf of SUD Life in connection therewith, to any person other than a person employed by the Service Provider in the performance of the Contract. Disclosure to any such employed person shall be made in confidence and shall extend only as far as may be necessary for purposes of such performance.
- The Service Provider shall not, without SUD Life prior written consent, make use of any document or information enumerated in this document except for purposes of performing the Contract.
- Any document, other than the Contract itself, shall remain the property of SUD Life and shall be returned (in all copies) to SUD Life on completion of the Service Provider's performance under the Contract, if so, required by SUD Life.
-

Trademark used under licence from respective owners.

6.11 Continuity of business

SUD Life requires a vendor to present a plan that specifically addresses what type of resources, how long and what load capacity will be available to ensure continued service in the event of a disaster.
Participants shall provide details of the Disaster Recovery & Business Continuity Plan (BCP).

6.12 Disposition of responses

All materials submitted in response to this RFP shall become the property of SUD Life.

6.13 Termination

SUD Life can terminate the agreement without assigning any reasons by giving three months' notice and is not liable to pay any penalty to the service provider on termination for any reasons

Trademark used under licence from respective owners.

ANNEXURE – A

Requirements & Details

Pre-Qualification Criteria/ Eligibility Criteria:

Sr. No.	Eligibility Criteria	Documents to be submitted	Compliance (Yes/No)
1	The Bidder must be an Indian Company/ LLP /Partnership firm registered under an applicable Act in India.	Certificate of Incorporation issued by Registrar of Companies and full address of the registered office along with Memorandum & Articles of Association/ Partnership Deed	
2	Bidder should have experience of minimum 05 years in providing the Software Solution/services	Copy of the order and/or Certificate of completion of the work. The Bidder should also furnish a user acceptance report	
3	Client references and contact details of customers for whom the Bidder has executed similar projects in India	Bidder should specifically confirm on their letterhead in this regard	
4	Certification Requirements SOC 1, SOC 2, SOC3, ISO 27001	SOC-2 and ISO-27001 standard Valid Certificate to be provided mandatorily	
5	OEM should have a support center and level 3 escalation (highest) located in India	Brief details information mandatorily	

SUD Life reserves the right to change the RFP Eligibility Criteria at any time prior to the opening of the commercial bid.

Trademark used under licence from respective owners.

SCOPE OF WORK

The bidder shall establish and configure the End-to-End DevSecOps Platform within the SUDL's on-premises or cloud infrastructure to align with the SUDL's specific needs. Platform should include a blend of DevSecOps tools.

Bidder will ensure successful execution of the mentioned activities for streamlined DevSecOps CI/CD pipelines implementation & operations in the SUDL throughout Continuous Planning, Continuous Development, Continuous Monitoring, Continuous Operations and Feedback, creating a comprehensive and robust DevSecOps Platform.

Objectives

Bidder is required to supply, deploy and maintain the DevSecOps continuous Integration (CI) /Continuous Deployment (CD) pipelines and ecosystem. Bidder to supply the licenses and solution as required based on the enterprise support model and required to extend full support during the project period covering various stages of the DevSecOps Process. Bidder will also be required to ensure integration of DevSecOps pipeline with other tools of the SUDL as specified in the RFP and any inter-integration between the tools within the supplied solution.

Bidder is to install, configure and commission the solution setup in Production DC, DR and UAT Environment. SUDL will provide the necessary infrastructure (Server, OS, DB (only Oracle DB)) required to install, configure, and commission the solution, though the sizing and solution architecture including Server, OS, DB, Middleware and deployment of the same will be taken care by the Bidder. Bidder is required to provide support for the implementation /migration of all the applications identified by the SUDL and bidder during assessment and planning phase.

Deliverables

Bidder will ensure to perform below mentioned activities to streamline DevSecOps CI/CD pipelines implementation & operations in the SUDL, broadly covering following services and functionalities:

Assessment and Planning Phase:

1. Bidder will have to conduct a thorough assessment of the existing software development practices and security practices, including a review of the SDLC, current security measures, and tooling landscape.
2. Bidder will have to collaborate with stakeholders, including software developers, security teams, IT operations, etc. to define project goals, objectives, and success criteria.
3. Bidder will have to analyse the existing infrastructure and identify any required necessary upgrades or modifications to support the DevSecOps implementation.

Trademark used under licence from respective owners.

4. The bidder would be responsible for requirement gathering, analysis and creating high level design and simulation of the solution which would be scalable, flexible while ensuring minimal manual intervention.
5. Bidder will have to develop a detailed Design Document containing details of solution architecture, integration architecture, workflows designs, infrastructure architecture, security architecture, CI/CD Pipeline(s) etc.
6. Bidder while developing detailed Design Document, shall finalize list of applications that can be on-boarded on DevSecOps Platform and will develop a plan for on-boarding and implementation of applications in DevSecOps environment
7. Bidder will have to develop a detailed Design Document along with Plan of action (POA) including roadmap for the DevSecOps Implementation, outlining key milestones, deliverables, timeliness, resource requirements, etc.
8. Design Document along with Plan of Action (POA) will have to be duly vetted by OEM
9. Assessment report containing Design Document along with Plan of Action (POA) will require acceptance from SUDL side, before initiating implementation.

Infrastructure Setup and Configuration:

1. Bidder will have to design and deploy infrastructure such as OS, Server, Database, Middleware, networks, storage component or SUDL's cloud setup etc. for the DevSecOps environment including hardening and closure of the VAPT observations. SUDL will provide Basic Infrastructure such as Server, OS License, Oracle Database (DB other than Oracle to be provided by the respective bidder)
2. Bidder will have to implement robust backup and disaster recovery mechanisms to safeguard critical DevSecOps infrastructure components and data.
3. Bidder shall be responsible to Integrate the chosen enterprise DevSecOps tools into the infrastructure, ensuring seamless interoperability and adherence to industry best practices for tool integration.

Tool Customization and Integration:

1. Bidder will have to deploy and create the DevSecOps CI/CD pipelines as mentioned in the RFP
2. Bidder will have to customize and configure the selected DevSecOps tools to align with our organization's specific requirements, including workflow design, integration with existing systems, automation settings, etc.
3. Bidder will have to coordinate and integrate the CI/CD pipelines with existing tools available with the SUDL as mentioned further in Scope of Work.
4. The solution should be implemented with appropriate authentication, access controls, and role-based permissions for tool usage to ensure secure access and protect sensitive data.
5. The solution should establish automated data flows and synchronization between tools to enable seamless information sharing and streamline the DevSecOps processes.

Process Implementation and Automation:

1. The Bidder will have to design and implement the solution with industry best practices, covering areas such as code development, code repository and version management, testing, vulnerability scanning, security reviews, deployment, monitoring, operations, feedback, etc.

Trademark used under licence from respective owners.

2. Bidder as part of the solution should have automated monitoring and alerting mechanisms via various modes but not limited to dashboard, server, email, SMS etc. should be integrated into the CI/CD pipelines to detect and respond to security incidents promptly utilizing relevant tools.
3. Bidder will integrate feedback loops and metrics into the processes to measure the effectiveness of the DevSecOps implementation, enabling continuous improvement.
4. Bidder will be responsible for Onboarding of applications identified during the **Assessment and Planning Phase.**

Training & Knowledge Transfer:

1. Bidder should conduct comprehensive training sessions for SUDL's staff, including developers, security team, operations teams etc. to familiarize them with the newly implemented DevSecOps practices and tools.
2. Bidder should provide detailed documentation, guides, and resources to support ongoing learning and knowledge transfer, including best practices, troubleshooting guides, and tool usage documentation.
3. Bidder should provide training to key personnel of SUDL to facilitate the adoption and successful implementation of the DevSecOps practices.

Validation and Continuous Improvement:

1. Bidder will have to deploy the solution using industry best practices such as hardening and must close all the VAPT Observations, VAPT will be conducted by the SUDL.
2. Bidder will conduct vulnerability assessments, penetration testing, security audits etc. to identify any potential weaknesses or vulnerabilities in the system and address them promptly.
3. Bidder will establish a framework for continuous improvement, incorporating regular reviews, feedback mechanisms, iteration cycles, etc.to refine the DevSecOps implementation based on lessons learned and changing requirements.
4. Bidder needs to collaborate with SUDL's internal teams to identify and implement enhancements, updates, and patches to the DevSecOps infrastructure to address emerging security threats and industry advancements.
5. Bidder needs to identify and implement enhancements, updates, and patches to the DevSecOps tools to address emerging security threats and industry advancements.

Monitoring & Management Services:

1. Bidder will have to provide 24x7x365 monitoring and incident management for the DevSecOps platform, ensuring prompt detection, response, and resolution of any issues or security incidents.
2. Bidders should perform routine maintenance tasks, including patching, upgrades, and performance optimization etc. to ensure the stability and optimal performance of the infrastructure.
3. Bidder should conduct capacity planning and scalability assessments to accommodate future growth and evolving business needs.
4. Bidder will have to maintain documentation and configuration records of the DevSecOps infrastructure, including network diagrams, system configurations, security settings, etc.
5. Bidder shall coordinate with relevant vendors for hardware and software maintenance, license renewals, and support escalations, as necessary.

Trademark used under licence from respective owners.

6. Bidder will have to provide regular reports and updates on the status of the infrastructure, performance metrics, and incident resolution activities.
7. Stay updated with the latest industry trends, security vulnerabilities, and best practices in DevSecOps and onsite technical support to proactively address emerging challenges.
8. Detailed Roles, Responsibilities, and other requirements related to OTS are mentioned in the subsequent sections of the RFP.

In addition to all the above points, bidder should provide the below deliverables but not limited to:

1.	Design Document along with Plan of action (POA)	As detailed in Assessment and Planning above.
2.	DevSecOps Solution Setup and Configuration	Bidder is responsible to install, configure, commission, Implementation DevSecOps environment, CI/CD Pipeline(s) and tools in UAT, DC, DR and will provide High Level and Low-Level Design Document to the SUDL before on-boarding of applications.
3.	Integration and on boarding of Applications	Bidder is responsible for onboarding of the application on DevSecOps CI/CD Pipelines and need to submit the application integration document covering details of integration, setup, configuration etc. including steps to conduct the DR Drill.
4.	Training	Bidder to submit the training calendar and training contents.
5.	Risk Management Plan	This document should outline the strategy for identification and mitigation of various type of risks like technical risks, security risks, confidentiality, privacy risks, etc.
6.	Performance Metrics	This document should include key performance indicators and metrics employed to evaluate the performance of the various tools as well as solution as whole.
7.	Security Plan	This document should include details of the security standards and security mechanisms deployed in the solution for ensuring the security of the solution and underlying data.
8.	Project Status Report	Bidder should provide a detailed report on supply, installation, implementation & migration to enable SUDL to keep track and update of the project progress.
9.	Yearly Assessment Report	This report shall contain the plan of action for remaining applications to be integrated apart from the applications identified during the Assessment and Planning phase (which are not implemented yet) as per SUDL's guidelines at the end of every year during the contract period along with assessment of changes, feasibility of automation and improvement in existing

Trademark used under licence from respective owners.

		setup
10.	Project Support Report	This report should provide details of MIS related to the day-to-day operations, failure of deployed processes with reasons and action taken, backup reports, periodic restorations report etc. This report shall be provided on Monthly Basis.
11.	Business Continuity Plan	This document should have a detailed plan for recovery of critical operations/processes of the solution in the event of a disaster. The plan should encompass complete backup and restoration procedures to minimise downtime and data loss.

All related documents, manuals, catalogues, and information furnished by the bidder shall become the property of the SUDL. Detailed documentation, and SOP's (Standard Operating Procedure) on activities such as DR Drill, Pipeline creation, application on boarding etc. should be submitted before project signoff.

Implementation

1. The entire solution supplied under this RFP must be installed, implemented, commissioned, and configured by Bidder / OEM. Bidder must submit the design document and an implementation confirmation report vetted by OEM comprising of, that all the points in the design document have been implemented. The bidder to make necessary arrangement for the same and SUDL will not pay any additional cost for implementation/configuration/architecture validation.
2. The bidder should arrange one technical resource of respective OEM/OSD to oversee the DevSecOps solution implementation during the implementation period without any cost to the SUDL.
3. Bidder should take full ownership for installation, implementation, commissioning, and configuration of OS (Linux / Windows, Database, Middleware, backup, Storage or any other required software) etc. as per applied application on DevSecOps solution during for solution setup and period for on-site setup.
4. The successful bidder has to ensure on-site support for resolving all solution related issues, including re-installation, reconfiguration of OS, Middleware, database, storage and other required software for the proposed solution, during entire implementation period.
5. The OEM/OSD should assign one technical resource to oversee the DevSecOps solution implementation during the implementation period.
6. If any Software /Hardware updates are provided by the OEM/Bidder, it should be installed & configured by the successful bidder during entire contract period without any additional cost to the SUDL.
7. Validate the completion of the prerequisites including patching and upgradation of CI/CD pipelines and ensure documenting the prerequisites before performing the activity.
8. Bidder shall be responsible for creating/customizing, configuring, implementing any new workflows and/or CI/CD pipelines as per the requirement of the SUDL during contract period, without any cost
9. Bidder shall be responsible to integrate/on-board any new application(s) in the DevSecOps solution using CI/CD pipeline(s) as per the requirement of the SUDL during contract period, without any cost

Trademark used under licence from respective owners.

10. SUDL may opt for Audit through third party Authorized Agency or by the SUDL officials for the supplied hardware and Software. Successful bidder is required to coordinate with the SUDL Officials & Audit agency to execute relevant test cases.
11. If there is any gap in interpretation of SUDL's requirement and bidder understanding for proposed solution, it will be the responsibility of Bidder to fill up the gap on time without any extra cost to SUDL during implementation of Project.
12. Custom Role Based Access Control (RBAC) for user group/ roles creation for all offered solutions under the RFP.
13. The bidder should provide requisite skilled resources without any additional cost to SUDL, during the implementation period.
14. The Bidder to maintain the code base of each microservices as a separate code repository, with best practices such as branches, tagging, etc.
15. The Bidder to ensure all deployments across environments (UAT, Production & DR) are directed through robust DevSecOps Tools following stage-gated quality controls. More environments could be set up as per the requirement of the SUDL at no additional cost to the SUDL.

Solution Capabilities

The DevSecOps Solution offered by the Bidder shall support following services and functionalities (including but not limited to):

Continuous Planning tool(s)

Continuous Planning Tool should enable the stakeholders to gather the requirements and feedback required to deliver the project during the initiation phase of the project.
Its purpose is to construct a clear product roadmap that guides future development endeavors. The tools must cater below requirements (but not limited to):

1. **Agile project management capabilities:** Agile methodologies, user story management, sprint planning, and backlog management.
2. **Collaboration and communication tools:** Integrated chat, discussion boards, and document sharing to facilitate collaboration among team members.
3. **Task tracking and prioritization:** Ability to create, assign, and track tasks, set priorities, and monitor progress.
4. **Integration with source control and CI/CD tools:** Seamless integration with source control and CI/CD tools to link tasks with code changes and automated build processes.
5. **Real-time reporting and analytics:** Dashboards and reports to provide visibility into project progress, team performance, and metrics.

Trademark used under licence from respective owners.

6. **Resource allocation and capacity planning:** Tools that provide resource allocation capabilities and help with capacity planning to ensure efficient project execution.
7. **Agile metrics and analytics**: Advanced analytics and metrics that provide insights into team performance, sprint velocity, and backlog forecasting.

Continuous Development tool(s)

It should support an efficient and streamlined software development lifecycle by providing the below-mentioned key features. The tools must cater below requirements (but not limited to):

1. **Code Scaffolding:** Offer reusable templates and scaffolding code to accelerate the bootstrapping of application development processes, reducing development time and effort.
2. **Multi-Language and IDE Support:** Facilitate development in all programming languages and seamlessly integrate with all Integrated Development Environments (IDEs) such as Spring Boot, .NET Framework, .NET Core, Node.js, Microsoft Visual Studio, Aptana Studio 3, PyCharm, PhpStorm, DataGrip, DbVisualizer, Codenvy, IntelliJ IDEA, WebStorm, NetBeans etc., catering to diverse project needs.
3. **Unit Testing and Error Reporting:** Enable Unit Testing and integrity checks to ensure code quality and provide version-wise bug/error reporting to help identify and address issues early in the development cycle.
4. **Version Control Integration:** The provided version control tool should be integrated with the other provided CI/CD pipelines to enable efficiently track changes, foster collaboration among developers, and maintain code consistency. To align with SUDL's requirements, please ensure that the chosen tool for source control and version control in the CI/CD pipeline aligns with the options listed by the SUDL.
5. **Integration Testing:** Offer provisions for integration testing, allowing developers to test how different components work together, ensuring smooth interoperability between different parts of the application.
6. **Automated Builds:** Automate the process of building the application from source code, reducing manual effort, and ensuring consistency in the build process.
7. **Continuous Feedback and Collaboration:** Facilitate collaboration among team members by providing features for code reviews, code approvals, comments, and discussions, allowing continuous feedback to improve code quality and promote knowledge sharing.
8. **Support for Continuous Integration (CI):** Seamlessly integrates with CI tools to enable automated builds, tests, and code integration, ensuring that changes are smoothly incorporated into the shared repository.
9. **Documentation Generation:** Provide options for generating and updating project documentation, aiding developers in maintaining accurate and up-to-date project information.
10. **Flexibility and Customization:** Allow developers to customize workflows, configurations, and preferences to suit project-specific requirements and development practices.

Continuous Integration tool(s)

It should streamline the development process by automating the integration of code changes from multiple developers into a shared repository. It should enable frequent and automated builds, tests, and deployments, ensure code quality and reduce the risk of integration conflicts. Additionally, the tool should provide real-time feedback to developers, allowing them to address issues promptly and maintain a reliable and efficient development workflow. The tools must cater below requirements (but not limited to):

1. **Centralized repository for storing and managing build artifacts:** A repository to store and manage build artifacts, libraries, and dependencies.

Trademark used under licence from respective owners.

2. **Versioning and dependency management:** Version control and dependency management to ensure consistent builds and deployments.
3. **Access controls and permissions management:** Control access to artifacts based on roles and responsibilities.
4. **Integration with CI/CD pipelines:** Seamless integration with CI/CD pipelines for artifact management and deployment automation.
5. **Artifact promotion and release management:** Processes and workflows to promote artifacts from development to production environments while managing releases.
6. **Dependency vulnerability scanning:** The provided continuous integration tool should get integrated with other CI/CD pipelines as per the RFP which will help to identify the dependencies and remediate security.
7. **License compliance management:** Tools that assist in managing and ensuring compliance with enterprise licenses and third-party dependencies.
8. **Artifact promotion workflows:** Workflows that define the promotion of artifacts across different environments with appropriate approvals and validations.
9. **Automated build and test execution triggered by code changes:** Automatic triggering of builds and test execution when code changes are pushed to the repository.
10. **Parallel and distributed builds:** Ability to parallelize and distribute builds to optimize build times and resource utilization.
11. **Integration with code analysis and testing tools:** Integration with code analysis and testing tools to provide continuous feedback on code quality and test results.
12. **Continuous feedback and notifications:** Real-time feedback and notifications on build and test results, ensuring immediate visibility into the codebase health.
13. **Parallel test execution:** Ability to run tests in parallel to reduce test execution time and accelerate feedback.
14. **Containerization support:** Integration with containerization platforms for building and testing applications in containers as and when required by the SUDL.
15. **Continuous Integration (CI):** Automating CI for the frequent merging of code changes, builds, and unit tests. It ensures that code changes from multiple developers integrate smoothly and reduces integration issues.
16. **Dependency Management:** Automatic dependency management ensures that the project uses secure and up-to-date libraries and frameworks. It checks for vulnerabilities and updates dependencies as needed.
17. **Build Artifact Management:** Storing and versioning build artifacts to enable traceability and reproducibility, to ensure that the exact build used for testing and deployment can be identified and retrieved.

Continuous Deployment tool(s)

It should automate the process of releasing code changes into various environments such as UAT, Production etc. rapidly and reliably. It should seamlessly integrate with the Continuous Integration CI/CD pipelines, ensuring that the tested and approved code is automatically deployed to the target environments without manual intervention. The tool should provide rollback capabilities in case of any issues and offer extensive monitoring and logging to ensure smooth and error-free deployments. Its goal is to enable frequent and safe software releases, enhancing the development team's agility and delivering value to end-users efficiently. The tools must cater below requirements (but not limited to):

Trademark used under licence from respective owners.

1. **Continuous Deployment (CD):** Automating the deployment process to enable frequent and reliable releases to production environments to reduce manual errors and ensure consistent deployment procedures.
2. **Infrastructure as Code (IaC):** Automate infrastructure provisioning through code to ensure consistent, reproducible deployments, treating infrastructure as software. This approach enables versioning, testing, and scalability.
3. **Configuration Management:** Separating application configuration from the codebase to manage and control configuration changes and to ensure versioning, auditing, and rollback of configuration settings.
4. **Secure Configuration Baselines:** Establish and maintain secure configuration baselines for operating systems, databases, web servers, and other infrastructure components which define security-hardened configurations to reduce the attack surface and ensure compliance with industry standards.
5. **Configuration Drift Detection:** Implement tools and processes to detect configuration drift, which occurs when the actual configuration of a system deviates from the desired or baseline configuration. Configuration drift detection to identify unauthorized changes, vulnerabilities, and inconsistencies.
6. **Secret Management:** Utilize a secure and centralized secret management solution to store and manage sensitive information, such as passwords, certificates, etc. Securely managing secrets to be ensured to reduce the risk of accidental exposure or unauthorized access.
7. **Continuous Compliance Monitoring**: Implement continuous compliance monitoring tools that can assess the compliance of configurations against regulatory requirements, security standards, and internal policies. Automated compliance to maintain a secure and compliant configuration posture.

Continuous Testing tool(s)

Bidder will be responsible for integrating the proposed tools, provided under this RFP for DevSecOps, with the SUDL's existing as well as future testing (security testing, functional testing etc.) tools, as applicable, as per the requirement of the SUDL, without any cost to the SUDL.

Continuous Operation & Feedback tool(s)

It should facilitate the capture of feedback and provide analytical capabilities to analyse the feedback, enabling data-driven decisions to shape future product development and enhancements. The tools must cater below requirements (but not limited to):

1. **On- Call Schedule:** Provide on-call schedule management for users to ensure availability of services is maintained.
2. **Escalation Policies:** Implement escalation policies to ensure missed critical alerts are captured well and next responder gets escalated in case first level resolution is not achieved.
3. **Data Capture and Retention**: Securely capture and store system and network data for in-depth post-incident analysis, facilitating a comprehensive understanding of the incident's scale and repercussions.
4. **Incident Alerting:** Implement an immediate response mechanism where email, SMS notifications are provided for triggered alerts.
5. **Incident Management:** Implement incident management process as per the SUDL Guidelines
6. **Change Management:** Implement a structured change management process as per the SUDL Guidelines.
7. **Feedback Loop:** Create mechanisms to gather feedback from users, developers, and operations teams which include user surveys, feedback forms, or monitor user forums and support channels to help identify improvement areas, collect feature requests, and address usability or performance issues.

Trademark used under licence from respective owners.

8. **Performance and Health Metrics:** Collect and analyze performance and health metrics of the application and infrastructure, such as CPU usage, memory utilization, latency, response time, integration latency, query fails/delay etc. to provide insights into system behavior, resource utilization, and capacity planning.
9. **Root Cause Analysis:** Implement a structured Root Cause Analysis process as per the SUDL guidelines.
10. **Continuous Feedback Mechanisms:** Establish channels for continuous feedback and collaboration between various teams such as development, security, operations etc to enable iterative improvements, knowledge sharing, and alignment of goals and priorities.

Continuous Monitoring tool(s)

It should automate the alert generation via various mechanisms but not limited to dashboard, email, SMS and should be integrated into the CI/CD pipelines. The tools must cater below requirements (but not limited to):

1. **Real-time Log Analysis:** Implement real-time log streaming to monitor events as they occur to ensure immediate visibility into application behavior, security incidents, and operational issues for timely response.
2. **Log Search and Filtering:** Powerful search and filtering capabilities to ensure quick retrieval of specific log entries or patterns for efficient troubleshooting, root cause analysis, and compliance auditing.
3. **Alerting and Notification:** Set up alerts and notifications based on predefined thresholds or specific log patterns for proactive monitoring and timely response to critical events or anomalies. Customizable alerting mechanisms to ensure relevant stakeholders are notified promptly.
4. **Anomaly Detection:** Apply machine learning algorithms or rule-based approaches to detect anomalous log patterns or behaviors for identifying potential security incidents, system abnormalities, or performance issues.
5. **Log Retention and Archiving:** Establish a log retention and archiving strategy to comply with regulatory requirements and enable historical analysis to ensure long-term storage and retrieval of logs for auditing and investigations as per the SUDL requirement.
6. **Event Forwarding:** The Capabilities within the platform to transmission data from diverse sources, encompassing host scanning, benchmarking, and runtime events, to third-party SIEM (Security Information and Event Management) platforms and logging tools ensuring the long-term retention of data logs and events.
7. **Request and Response Capture:** Capture detailed information about API requests and responses, including headers, payloads, and timestamps to facilitate thorough analysis and troubleshooting of API interactions.
8. **Transaction Monitoring**: Monitor and trace API transactions across microservices or distributed systems to provide end-to-end visibility into the flow of requests, helping to identify bottlenecks, track requests, and diagnose issues.
9. **Performance Metrics**: Collect and analyze performance metrics such as response time, latency, and throughput for individual API calls.
10. **Distributed Tracing**: Implement distributed tracing techniques, such as correlation IDs or distributed tracing frameworks, to trace requests across multiple services and components enable end-to-end visibility into complex API architectures and facilitate troubleshooting in microservices environments.
11. **API Dependency Mapping**: Automatically generate and maintain a map of API dependencies within the application ecosystem to help understand the impact of changes, identify dependencies, and ensure accurate tracking.
12. **Error and Exception Tracking**: Capture and track errors and exceptions that occur during API interactions to enable proactive identification and resolution of issues, improving application reliability and stability.

Trademark used under licence from respective owners.

13. **API Versioning and Compatibility Checks**: Implement mechanisms to manage API versions and ensure backward compatibility to help prevent breaking changes and ensure smooth transitions and deployments.

The Continuous Security Tool(s)

Bidder will be responsible for integrating the proposed DevSecOps tools, being provided under this RFP, with the SUDL's existing as well as future Security tools, as applicable, as per the requirement of the SUDL, without any cost to the SUDL.

The Container Registry Tool(s)

The proposed DevSecOps CI/CD pipelines should be able to integrate with all the leading Container tool(s) which could be made available by the SUDL in the future.

Additional Features

1. Development of software applications project should be done using management methodology such as agile/waterfall etc.
2. Deployment of application architectures based on Monolith, SOA based, as well as Microservices etc.
3. Development using multiple technologies i.e., Java, .NET Framework, .NET
4. Implementation of the DevSecOps CI/CD pipelines with CI/CD tools should be in line with the DevSecOps Maturity Model advance stage.
5. The CI/CD pipelines should be able to cover all Web Apps, Mobile Apps, and other applications of the SUDL.
6. The platform must offer a unified and comprehensive reporting dashboard, encompassing "continuous measurement," empowering the SUDL to monitor and assess the adoption and implementation progress effectively.
7. The solution should have the capability to seamlessly integrate existing enterprise applications such as (Finacle, Internet SUDL, Mobile SUDL, API Gateway, FI Gateway, CKYC, eKYC, DMS, etc.) with the DevSecOps CI/CD pipelines, encompassing various activities such as version control, security practices, and build/deployment processes.

Trademark used under licence from respective owners.

Toolset & Software

1. SUDL envisions the following tools for the End-to-End DevSecOps CI/CD pipelines where the bidder is required to choose from the identified list to provide a standard set of tools that could be used to create seamless CI/CD pipelines and can support and deliver all functionalities of DevSecOps ecosystem.
2. It should comprise of Software tools based on Enterprise Support model/Licensed tools.
3. It is the bidder's responsibility to ensure that software tools are carefully selected and along with their services, the entire scope is compressively covered to meet the objectives of the RFP.

DevSecOps Primary Area	DevSecOps Sub Area	Identified Tool Set	License/ Support Metric
Continuous Planning	Planning Management	Jira Data Center / Gitlab Self-Managed+ / Azure DevOps	Enterprise Version
	Threat Modelling	Provided By SUDL	Enterprise Version
Continuous Development	Source Control	Bitbucket Data Center / GitLab Self-Managed+ / GitHub Enterprise Server	Enterprise Version
	Coding	Visual Studio/ Eclipse/ JetBrains IntelliJ	Enterprise Version
	Unit Test	Junit, Nunit, PYTest	Enterprise Version
Continuous Integration (CI)	Manage Artifacts	Sonatype Nexus/ Jfrog/ Harbor	Enterprise Version
	Secure Code Analysis	Provided by SUDL	Enterprise Version
	Static Code Analysis		Enterprise Version
	Build	Maven/ Ant	Enterprise Version
	Integration/ CI	Jenkins/ GitLab/ Azure DevOps	Enterprise Version
Continuous Functional and Security Testing	Functional Testing	Testing Center of Excellence (TCoE) tools will be used for testing related areas of DevSecOps. Provided by SUDL	Enterprise Version
	Non-Functional Testing		Enterprise Version
	Integration Testing		Enterprise Version
	API Testing		Enterprise Version
	Performance Testing		Enterprise Version

Trademark used under licence from respective owners.

Continuous Deployment (CD)	Configuration	Puppet/ Chef/ Ansible Tower	Enterprise Version
	Deploy/CD	Jenkins/ GitLab/ Azure DevOps	Enterprise Version
Continuous Monitoring	Logs monitoring	ELK/ AppDynamics/ Splunk	Enterprise Version
	Application Monitoring	Dynatrace/ Grafana Enterprise/ AppDynamics/sysdig	Enterprise Version
	Infrastructure Monitoring	AppDynamics/ Dynatrace/ Sysdig	Enterprise Version
	API Tracing	Kubernetes ServiceMesh/ Charles Proxy/ ELK/ Dynatrace	Enterprise Version
Continuous Feedback	Feedback	Jira service management/ Ops Genie/GitLab-Self Managed	Enterprise Version

4. The SUDL prefers establishing a DevSecOps platform and currently possesses several tools to cover various aspects, including SCA (Software Composition Analysis), SAST (Static Application Security Testing), and DAST (Dynamic Application Security Testing). Therefore, the chosen bidder, with their proposed platform or solution, should demonstrate the capability to effectively integrate and utilize the existing tools already in use by SUDL.
5. Currently SUDL is using TFS (Team Foundation Server) for code repository, Bidder to migrate all the existing code repository from TFS to proposed solution.

Hardware/Software Sizing

1. Bidder should submit the sizing of infrastructure required for deployment of the DevSecOps CI/CD Pipelines including server, OS, DB with technical bid document at the time of bid submission.
2. Solution should preferably be hardware, OS and DB agnostic in nature. SUDL shall provide the complete infrastructure hardware as per the sizing shared by the successful Bidder and shall be responsible for its AMC renewal, Support and maintenance.
3. The Bidder shall be responsible for installation, re-installation, configuration, setting up, implementation, monitoring and support of all the components of the DevSecOps solution in DC, DR, UAT including the components being provided by the SUDL.
4. Bidder should provide the details of Database and Middleware required to complete the solution, if Oracle is not the chosen database and WebLogic is not the chosen middleware, then bidder should provide the database & middleware for the complete solution setup (DC, DR. UAT).
5. Any software and/or tool other than proposed solution required to complete the solution shall be provided by the bidder.
6. Bidder should ensure to size the hardware as per SUDL's requirement mentioned in the RFP to adhere the SLA, and there should not be any performance issue during the complete tenure/contract period. Bidder should ensure all the CPU utilization of any server/ appliance should not go beyond 70% in the complete tenure of contract.

Trademark used under licence from respective owners.

7. The platform/solution should be able to support minimum of 300 Active Users with the ability to further scale up in terms of number of active users at a given time.
8. The details of sizing of infrastructure required for the DevSecOps Solution to be submitted by the bidder as per the format given in Annexure -25 Format for submitting the sizing of infrastructure required for the DevSecOps Solution.

Infrastructure

1. The proposed solution shall be hosted initially on the SUDL's on-premises. However, the solution should have the capability to migrate to any other infrastructure including private cloud and public cloud as per the SUDL's requirement. The SUDL shall provide necessary infrastructure such as Servers, operating system, Oracle database etc. which shall be managed by the Bidder during the entire contract period under the SUDL's supervision.
2. The successful bidder must design the solution with high availability & secure infrastructure in the Data Centre and disaster Recovery site as per industry-accepted security standards and Best Practices.
3. The platform should be able to on-board and support applications developed using Micro-Services Architecture and deployment of container-based platforms as and when adopted by SUDL.
4. The SUDL will provide the necessary set infrastructure, any other software to be used needs to be configured by the successful bidder apart from the already in-use software provided by the SUDL.

Regulatory & Security Requirements

As defined in the SUDL's Policy and guidelines from time to time. The solution deployment will be subject to Security review. Bidder must ensure compliance with the regulatory guidelines and SUDL's Policies, some of which are as under:

1. Password Policy of the SUDL.
2. Data Encryption/ Protection requirement of the SUDL.
3. The solution should comply with all security certifications and regulatory requirements of the SUDL (VAPT, OS/Application/Database SCD, DLP, risk assessment, etc.) as per policy to ensure data consistency and data security.
4. The solution should adhere to the security policies set up by the SUDL. The bidder must ensure that the solution complies with regulatory and statutory requirements of SUDL.
5. The solution must comply with data sharing policies and regulations and ensure data is shared is shared only with authorized parties and departments.
6. The Bidder shall not disclose or use any information given access to, by the SUDL, during the entire tenure of the contract, with any third party.
7. The bidder shall ensure the privacy and security of the SUDL's data or customer's sensitive data processed, stored, or transmitted over the solution and underlying IT infrastructure, including public cloud infrastructures (if involved), as well as provide necessary security and access controls and permissions.
8. The solution should comply with data protection and data localization norms.
9. Necessary Documentation on all the stages to be ensured by the bidder in coordination with the SUDL and the same to be provided to the SUDL

Trademark used under licence from respective owners.

Licenses

1. The bidder shall be responsible for procuring all the licenses in the name of the SUDL for the solution including all tools required for implementing the solution and furnishing the SUDL with all the licensed software/applications/tools developed or procured during the contract period. The Licenses provided to the SUDL should be of perpetual nature.
2. The bidder will be responsible for managing the licenses, ensuring compliance and tracking the license expiry dates and renewal requirements of the solution during the contract period.
3. The bidder shall assume full responsibility for any legal consequences that may arise from the infringement of patents, trademarks, or copyrights related to the solution supplied by the bidder to the SUDL.
4. SUDL shall not pay for Separate Licenses or Migration Cost in case of Movement from On Prem to Cloud or vice versa.
5. SUDL reserves the right to place order for any quantity for any of the line items (as per Annexure 16) as and when required by the SUDL, at the same rates and terms & conditions of initial contract, during the contract period.
6. SUDL is not bound to place any minimum order for any item.
7. Separate PO shall be placed each time for procurement of additional licenses, as and when required by the SUDL. Payment terms shall be derived by the respective PO released by the SUDL.

Business Continuity Plan

1. DC - DR synchronization for complete solutions (i.e. application configuration, CI/CD Pipelines etc.) should be made available as part of the solution so that in case of switch over the complete solution should be seamlessly working.
2. The bidder must ensure the DC-DR switchover and DR-DC Switchback are completed smoothly.
3. The bidder shall regularly test and update their BCP to test its effectiveness and accuracy.

Architecture

1. The proposed solution should have a multi-tiered architecture and should support microservices with complete functional and technical separation of processes, to ensure error free operations, scalability, maintainability, and optimal performance.
2. The solution should be cloud native, if the SUDL decides to move the solution to cloud it should be readily moveable.
3. The bidder should propose a solution, which should be flexible in deployment. Solution should support on-premises, cloud management, and hybrid models.
4. The solution should be compatible with physical, virtual machines and container-based deployments.

Trademark used under licence from respective owners.

High Availability

1. The solution must minimize the impact of single or multiple component/server/process/software failures in the production environment. It must ensure that the system can continue to operate without any significant disruption or downtime in the event of such failures.
2. The solution shall be designed with redundancy in mind to ensure zero impact by the failure of one or more components/servers or software in the production environment.
3. The bidder must take the backup of logs, audit trails etc. as per SUDL's policy. All other back-ups are to be maintained by the successful bidder as per the policy of the SUDL.
4. Log all administrative activities properly with a proper audit trail which should be capable of being used as forensic evidence.
5. Ensure 99.99% availability for the proposed architecture and an uptime of at least 99.95% for the proposed solution.
6. The platform should be architected to be fault tolerant and ensure cascading failure do not occur.

Maintenance & Support

1. The selected bidder must provide 24/7 support to the SUDL throughout the contract period, with an efficient escalation process and onsite technical support.
2. The Bidder shall provide patches/updates, and upgrades during the contract period and implement the same without any additional cost to the SUDL.

Governance Structure

The DevSecOps solution should have a strong governance framework in place to ensure appropriate usage, with clear policies and procedures for access, monitoring, and control.

Other Requirements

1. Offer isolation to micro services layer from the public facing API gateway layer. Inter- service communication should not take traffic out of the layer in which the services are hosted.
2. Provide Open APIs for integrations and conform to REST & SOAP API specifications.
3. Leverage modern DevSecOps practices for faster and more secure deployments of upgrades, patches, and release management.
4. There should be a review mechanism in the proposed solution for any addition, deletion, or modification requests.
5. The integration process will seamlessly connect tools and platforms with SUDL's Single Sign-On (SSO) solution, precisely tailored to meet the SUDL's specific requirements. The same shall extend to the SUDL's email and SMS systems, enabling the prompt delivery of relevant notifications and ensuring secure and efficient communication across systems, resulting in seamless user experience.
6. The platform must seamlessly integrate with the SUDL's cyber security platforms, including the Security Operation Centre (SOC) and Security Incident Event Management (SIEM) systems, Endpoint Security, and other applications.

Trademark used under licence from respective owners.

7. The bidder must provide the SUDL with all the code, scripts, and relevant material developed during the contract.
8. The solution (software/Application Software) provided by the successful bidder including the surrounding applications/software deployed by the Bidder, if any, should not be declared end of sale within 2 years of sign off the project. In addition, the solution provided by the successful bidder, including the surrounding applications/software deployed by the Bidder, if any, should not be declared end of support during the contract period and extension period, if any. If at all the solution or any Application Software is declared end of support within 5 years of project sign off, the successful bidder must provide & implement the upgraded version (software/solution) free of cost, to the SUDL.
9. Wherever CI/CD Pipelines is used in this RFP, it refers to the entire DevSecOps Pipeline from continuous planning to continuous feedback including continuous planning, continuous development, continuous integration, continuous testing, continuous security, continuous deployment, continuous monitoring and continuous feedback.

Onsite Technical Support

1. Administration & Management Service

a. Successful bidder should provide on-site support to the SUDL for Administration, maintenance & support of the End-to-End Solution for entire contract period.
b. The bidder's team should work on PNB Premises on general shifts or rotational shifts on need basis on all working days.
c. The bidder's team may be required to attend certain shifts on holidays/ off days / late evening hours, as and when required.
d. The escalation process of the bidder's team should be defined and in place for unresolved issues.
e. Bidder's support staff should be well trained to effectively handle queries raised to bidder.
f. The bidder's team to apply patches, new releases, upgrades, fixes, hardening, etc. to the DevSecOps platform as well as tools as decided by the SUDL.
g. Provide support to older versions of the software in case the SUDL chooses not to upgrade to the latest version.
h. Download and maintain a Central Repository of all the DevSecOps toolset installable, its latest patches, upgrades, fixes dependencies, etc. resolving the security findings and recommendations as decided by the SUDL.
i. Performing DC and DR Drill on periodic basis for the implemented solution which will include Hardware Infrastructure, Container Platform, Enterprise OS, DevSecOps Tools etc. as per SUDL's requirement.

2. Workplace Policy

a. During the contract, the bidder and the OTS Team shall at all times comply with & abide by the security policy of the SUDL, as the same may be applicable to or in respect of the works and the provisions of the contract.
b. Confidentiality of the infrastructure and application setup, configurations, and any related details shall not be disclosed by the successful bidder to any third parties or persons without SUDL permission.
c. OTS Team will follow and comply with the procedures and policies, applicable to the scope of work mentioned above, as per the SUDL's policies from time to time, and also extend full cooperation to

Trademark used under licence from respective owners.

the auditors designated by the SUDL in a way as they are expected to assist and cooperate for their audit.

d. The bidder shall provide backup resources in case any of the project members avail leave from the bidder's team.

3. Reporting

a. Bidder to perform server Administration, Health Monitoring of Servers, and maintenance of daily checklist in the format provided by the SUDL.
b. Bidder to perform Root Cause Analysis (RCA) of the incidents and reporting of Security incidents.
c. Bidder to Prepare and maintain Standard Operating Procedure (SOP) document pertaining to the services/Operations and should be updated whenever there is any change or addition is made.
d. Bidder to ensure SLA Maintenance / Management, monthly Uptime reports, utilization reports & interface utilization/reporting of all the devices.
e. Bidder to ensure Inventory Details to be kept available for the in-scope components including the underlying infrastructure.
f. Onsite Technical Support team shall publish reports to the SUDL team / management as per defined frequency but minimum twice in a day regarding real time factual status of all IT assets and uptime of the solution to be ensured.
g. Bidder to provide Escalation Matrix for the overall project and maintain the track of timelines of each milestone.

4. Support

a. Bidder to Support and work with the respective SUDL's teams to onboard them onto the DevSecOps platform for legacy as well as new-age applications or services by using the ticketing tool.
b. Bidder to guide the Application teams to deploy their application & related infrastructure configuration to UAT, Production DC & DR environments.
c. Bidder to guide and assist in on-demand requests from projects/departments of the SUDL for any expert troubleshooting of DevSecOps tools.
d. The Bidder will also provide suitable on-site technical staff to supplement the efforts of the OTS resources during emergencies/contingencies, which might impact the systems and services, covered under this scope.
e. OTS has to cover solving day-to-day issues while using the proposed solution in the SUDL's environment like resolving the issues related to Incidents, Security Threats, Signature/Pattern updates, Daily Updates, Product related Issues, and any other issues as per SOW/SLA at no extra cost to the SUDL.
f. OTS to ensure to keep the centralized DevSecOps setup safe from any security vulnerabilities and also adhere to any compliance as decided by the SUDL.
g. OTS team to Coordinate with all the teams for follow-up of open tickets & activities. Resolving technical issues & lodging tickets with OEM and following up on pending calls.
h. The bidder should communicate new features and upgrades as and when the new versions are available.
i. The bidder shall upgrade and/or customize the solution without any additional cost to SUDL whenever new version of software is released.

Trademark used under licence from respective owners.

5. Other Requirement

a. The SUDL may reduce/increase the manpower requirements during the project duration if workloads reduce/increase due to any reason.
b. Post-implementation - The transition plan, takeover process from the project team, and coordination with all the stakeholders should be performed by the OTS Team.
c. The OTS team has to prepare a patching calendar as per the frequency of the patches released by the OEM team, this is to be shared with the SUDL team.
d. All the OTS resources deputed at the SUDL should have a Background, qualification and experience verification report submitted by bidder's HR Head. The bidder needs to submit the qualification details & Background Verification and experience report of OTS resources along with all documents at the time of joining the onsite technical support team.
e. Current and Future requirements / Customizations required by the SUDL will be developed and deployed by the bidder without any additional cost to the SUDL.
f. SUDL reserves the right to interview the OTS Personnels including the Technical Lead intended to be deployed and if not found suitable may reject them.
g. Bidder to create and regularly update relevant documentation, such as detailed procedural documents about the processes, structure, access mechanism, deployment, etc. of the DevSecOps platform.
h. Services of OTS resources shall also be used for customizing and creating any new workflows and/or any number of CI/CD pipelines as and when required by the SUDL
i. OTS resources shall also be used to integrate/on-board any new application(s) in DevSecOps solution using CI/CD pipelines as per the SUDL's requirement.
j. Maximize the level of automation and self-service in the DevSecOps ecosystem.
Ensure Backup, Recovery, and DR of the DevSecOps platform as decided by the SUDL.
k. The bidder should provide quarterly preventive maintenance and health check report of the overall DevSecOps solution including all aspects of the solution such as infra, solution, usage, applications, compliance etc.

TECHNICAL Evaluation:-

The vendor to submit the following documents for technical evaluation.

- Latest 3-year Balance sheet and P&L
- Details of Client list
- Detail of Company Profile
- Details of Geographical Coverage
- PAN Card / Aadhar Card / Company incorporation letter / Partnership deed
- Memorandum of Association
- GST detail with Certificate
- Business Continuity Policy and Plan

Trademark used under licence from respective owners.

ANNEXURE – B

PROCESS COMPLIANCE STATEMENT

The following terms and conditions are deemed as accepted by you on participation.

1. You cannot change price or quantity or delivery terms (or any other terms that impact the price).
2. You cannot divulge either your Quotes or those of other suppliers to any other external party.
3. You agree to non-disclosure of trade information regarding the purchase, identity of buyer, process, documentation and other details.
4. In the event of your quote being selected by SUD Life and you subsequent default on your quote , you will be required to pay SUD Life an amount equal to the difference in your quote and the next selected by the buyer quote on one year's quantum of purchase (indemnity clause).
5. SUD Life's decision will be final and binding on you and will not necessarily be based on price. Though price is a very important factor of the decision-making.
6. Splitting of the award decision over a number of suppliers or over time (as in the case of staggered deliveries) will be at SUD Life's discretion.
7. You agree to furnish the techno-commercial compliance statement as per the enclosed format along with this statement.

I agree to have read, to understand and agree to abide by this statement. I agree to the fact that the information provided by my organization constitutes a legal, binding quotation. My quote is considered firm and reflects Star Union Dai-ichi Life Insurance's requirements stipulated in request for quotation (RFP).

Dated this ..... day of ..... 20....

_____ _____

(signature) *(In the capacity of)*

Duly authorized to sign Proposal for and on behalf of

_____

****

Trademark used under licence from respective owners.

ANNEXURE- C

TECHNO-COMMERCIAL COMPLIANCE STATEMENT

Clause No	Technical specifications/ commercial terms	Compliance (Yes/No)	Please indicate reasons in case of No and counter offer
1	Scope of Services		
2	Operating Days & Hours		
3	Selection Process		
4	Award Decision		
5	Service & Penalty		
6	Payment		
7	Order Cancellation		
8	Force Majeure		
9	Inspection and Audit		
10	Use of Contract Documents and Information		
11	Confidentiality		
12	Continuity of business		
13	Disposition of responses		
14	Termination		

I understand and agree to the fact that above information constitutes a legal, binding quotation. My quote is considered firm and reflects Star Union Dai-ichi Life Insurance's requirements stipulated in request for quotation (RFP).

Dated this ..... day of ..... 20....

_____ _____

(Signature) *(In the capacity of)*

Duly authorized to sign Proposal for and on behalf of

_____

****

Trademark used under licence from respective owners.

ANNEXURE –D

Cost Information

Cost information should be provided as per below

Option A

Sr No.	Description	Price
1.	Specific assessment. Ransomware Assessment Network Infiltration & Endpoint (Windows only) Attack Vectors WAF, Firewalls, EDR, and other security tools assessment. Number of Assessments: Two (02), with remediation and reassessments. One-Time Implementation and Integration Cost	

Option B (Full BAS Assessment)

Sr No.	Description	Price
1.	DevSecOps Solution Annual Subscription / Annual Technical Support cost, including all features. Unlimited assessment. One-Time Implementation and Integration Cost.	

Vendor should provide the details of terms & condition along with the applicable taxes %.

- All prices should be excluding applicable Taxes
- The quantity provided herewith is to ease vendors to arrive at unit cost for each slab.
- The above numbers may vary (decrease/increase) basis business requirement.
- Purchase Orders will be placed on actual business demand basis.

Trademark used under licence from respective owners.

PROPOSAL FORM (PRICE PROPOSAL)

Date: ……..

To:
Executive Vice President (Finance Controller),
Star Union Dai-ichi Life Insurance Company Limited
11th Floor, Raghuleela Arcade,
IT Park, Sector 30A,
Opp Vashi Rly Stn., Vashi
Navi Mumbai 400703

Dear Sir,

Re: Request for Proposal for DevSecOps Solution

having examined the Proposal Documents, the receipt of which is hereby duly acknowledged, we, the undersigned, offer to render services in conformity with the said Proposal documents for the sum of..... *(Total Proposal amount in words and figures)* or such other sums as may be ascertained in accordance with the Schedule of Prices attached herewith and made part of this Proposal.

We agree to abide by the Proposal and the rates quoted therein for the orders awarded by SUD life.

Until a formal contract is prepared and executed, this Proposal, together with your written acceptance thereof and your notification of award, shall constitute a binding Contract between us.

We undertake that, in competing for (and, if the award is made to us, in executing) the above contract, we will strictly observe the laws against fraud and corruption in force in India namely "Prevention of Corruption Act 1988".

We understand that you are not bound to accept the lowest or any Proposal you may receive.

Dated this ..... day of ..... 20….

_____ _____

(Signature) *(In the capacity of)*

Duly authorized to sign Proposal for and on behalf of

_____

****

Trademark used under licence from respective owners.