

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
1	26	Bidder's Eligibility Criteria -3	Point Nos 3 - Bidder should have experience of minimum _10__ years in providing the Services in field of IS Audit including Information Security audit. Bidder Should be Cert-In Empaneled and its empanel should be valid during the period of Services.	<ul style="list-style-type: none"> • Please confirm us number of work order to be submitted. Please confirm do we need to submit PO for each year. • We understand that if we are conducting security audit for 2 separate years for same organization under a single agreement / PO , the same will counted as 2 instances. Kindly confirm • Client certificate – Please confirm is it the completion Certificate 	1- Yes Invoice will be submitted annually.Audit will be divided in phases , Two or three phases (decided at the time of actual audit) and invoices will be issued post issuance of reports of each phases, consider phases as milestones.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
2			<p>Point 6- Education Qualification and Experience of a team: at least 2 resources and SME as and when required.</p> <p>1-Educational qualifications: Graduation in Electronics and Telecommunications or Computer Science or Information Security or Cyber Security or MCA</p> <ul style="list-style-type: none"> • Mandatory certifications: CISA/CISM/CISSP/OSCP/ OSCE (Minimum two) <p>2-Experience: Minimum 7 to 9 years of experience in BFSI domain in IS Audit including information & cyber security audit and have handled such assignments in the past for minimum 3 clients end to end from BFSI sector and subject to evaluation of proposed auditors' profile, by respective SBIL authorities during the actual assignment</p>	<p>We request you to relax the clause and ammend this with one certificate and also include iso27001 LA certificate</p>	<p>1- Educational criteria can not be relaxed</p>

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
3	32	Appendix-E	Scope of Work and Payment Schedule- 1. Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Not clear - Please elaborate more on scope of work	<p>1- Applications are divided in critical and non critical, for critical application will be audited every year and non critical in the span of 3 years.</p> <p>2- For example, if out of 100 applications, 40 are critical and 60 are non critical, then 40 critical + 20 (1/3 of 60 non critical) applications will be covered every year. As a audit scope when firms will review User access review, data for this application will be used to conclude observation.</p>

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
4	35	Appendix-F	Commercial Bid	Not clear - Please elaborate	<p>1- Total amount vendor will charge for conducting audit for 3 years (for ex, if INR 1 lakh is quoted for conducting audit of 60 application for each year 1,2, and 3 then 3 lakhs will be for 3 years.</p> <p>2- each year separately mention 2025-26- 1 lakh, 2026-27- 1 lakh and for 2027-28- 1 Lakh.</p> <p>2- This contract will be continued for 3 years basis performance at the end of year 1 and 2.</p> <p>3- If in any case more then 60 application to be audited in any given year , what would be extra amount will be charged per year per application that needs to be quoted separately.</p>
5	36	Appendix-H	NON-DISCLOSURE UNDERTAKING	<p>Please confirm following</p> <p>1. Do we need to submit along with the bid</p> <p>2. Do we need to submit on stamp paper.</p>	Post selection,NDA will be signed at the time of agreement on stamp paper it is a part of agreement.
6		Annexure	Annexure	We request you to provide us all annexure in word format	Will be provided

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
7	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Is any documentation review also under the scope of the engagement? If yes, what are expected number of documents to be reviewed during each year?	Yes, Document review will be a part of audit testing, in the process of auditing documents like Policies procedures, Application architecture High level and low level document, BRD documents etc will form part of the audit
8	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	What are the in scope locations and offices to be covered as part of the audit?	Sopped Location. 1- Head office at Natraj, Andheri. 2-CPC, Seawoods. 3- DR site located at Hyderabad 4- Any new site if required during audit.
9	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Is vendor required to conduct an application risk assessment for the applications or only an audit report with findings and recommendations would suffice?	It's an assurance assignment, Only walkthrough document, queries, Audit reports and recommendation as a part of report etc need to be prepared

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
10	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Please confirm if appropriate information security policies and procedures (Information Security, Business Continuity, Third Party Risk Management etc.) with respect to the organization are developed, established and available in the documented form.	Yes, Policies and Procedures are well defined and documented
11	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Please confirm if a risk register pertaining to the CIA (confidentiality, integrity and availability) requirements is in place or not.	Confidential details will be disclosed after selection and at the time of audit
12	Page 27	Appendix B - Bidder's Eligibility Criteria	Audit team shall be dedicatedly stationed at SBIL CPC Seawoods office for the period of Audit at the expense of Service provided.	What shall be the working mode for three years of engagement? Hybrid or entirely onsite?	Entirely Onsite at Seawoods and on some days at Andheri and one visit at DR site Hyderabad
13	Page 32	Appendix E - Scope of Work and Payment Schedule Point (d)	Firm shall provide an independent review and analysis of the organization's information security initiatives and objective assurance on Agreed Scope. Scope and objective of the information system (IS) audit is as per: (d) ISO 27001 framework.	Do you expect us to coordinate with a Accredited Third Party for certification? (such as ISO 27001:2022). If yes, then how many certifications are included as part of the scope of work.	No

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
14	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Does the scope also involve any audit of the DC/ DR sites? If yes, then how may sites are to be considered under the current scope of work.	yes one site at Hyderabad and if during any other site erupts during audit
15	Page 27	Appendix B - Bidder's Eligibility Criteria	Audit team shall be dedicatedly stationed at SBIL CPC Seawoods office for the period of Audit at the expense of Service provided.	vendor has considered onsite travel to the SBI Life Seawoods office only. Kindly confirm if our understanding is correct.	Yes onsite travel is at seawoods only and visit to DR Site
16	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Please confirm if any application to be considered in-scope are outsourced to a third party? If yes, please confirm whether the third party applications would form part of the scope of the assignment?	yes In scope application includes externally developed and serviced and on the shelf application will also for part of audit and included in scope of the audit
17	Page 27	Appendix B - Bidder's Eligibility Criteria	Audit team shall be dedicatedly stationed at SBIL CPC Seawoods office for the period of Audit at the expense of Service provided.	Vendor has considered only a 5 day work week for the engagement. Kindly confirm if our understanding is correct?	yes 5 days working

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
18	Page 27	Appendix B - Bidder's Eligibility Criteria	Bidder should have experience of minimum _10_ years in providing the Services in field of IS Audit including Information Security audit. Bidder Should be Cert-In Empaneled and its empanel should be valid during the period of Services.	Is Vendor required to provide client name as well in the proof of past 10 years of experience in providing services related to Information and Cyber Security Audits?	Yes it is required
19	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Please provide the number of cloud applications to be considered in-scope(within the total 100 applications scope), if any.	Confidential details will be disclosed after selection and at the time of audit
20	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	How many vendor applications approx. to be included as part of the audit?	Confidential details will be disclosed after selection and at the time of audit

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
21	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Separate audit reports are required to be developed for each application. Please confirm if our understanding is correct.	Audit can be conducted in phases to be decided post selection.
22	Page 32	Appendix E - Scope of Work and Payment Schedule	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Please provide the list of on-premise and cloud applications to be considered in-scope if any. Please provide the list of those applications/ products. And Please specify the name of the cloud service provider (CSP). And What is the cloud deployment model used in the organization for cloud applications? (Public, Private, Community, Hybrid)?	Confidential details will be disclosed after selection and at the time of audit
23	Page 36	Appendix G - Service Agreement	Appendix G - Service Agreement	We are not able to download/ open the service agreement template. Kindly share the document separately.	Will be provided
24	Page 12	9. BID PREPARATION AND SUBMISSION	A copy of board resolution or equivalent along with copy of power of attorney (POA wherever applicable) or equivalent showing that the signatory has been duly authorized to sign the Bid document.	Kindly mention why is the board of resolution required?	Board resolution to ensure authority signing audit report is actually authorised to sign report on behalf of firm.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
25	Page 12	9. BID PREPARATION AND SUBMISSION	A copy of board resolution or equivalent along with copy of power of attorney (POA wherever applicable) or equivalent showing that the signatory has been duly authorized to sign the Bid document.	Would a Letter of Authorization (LoA) on standard vendor letterhead suffice for this requirement?	Ok
26	Page 2	Schedule of Events	Last date and time for Bid submission: Up to 6:25 PM on 25th June 2025	Kindly extend the bid submission due date.	Extended till 8 July 2025 till 6:25 PM
27	Page 32	Appendix E - Scope of Work and Payment Schedule	The Auditing Team shall prepare an audit checklist based on above regulations, policy frameworks, guidelines, practices etc. within first month of the engagement. This checklist should clearly identify the references taken from whichever standard / regulation / framework etc. This audit checklist shall be verified by a SME and provide his / her sign-off to start the audit using this checklist.	Kindly confirm whether the approved audit checklist, post SME sign-off, is expected to be shared with SBI Life as a formal deliverable.	Yes
28	Page 32	Appendix E - Scope of Work and Payment Schedule	(i) COBIT (Control Objectives for Information Technology) of ISACA	Our assumption is that COBIT 2019 will be used as the reference framework for audit checklist preparation. Kindly confirm if our understanding is otherwise.	Yes Cobit 2019 will be used for reference purpose.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
29	Page 32	Appendix E - Scope of Work and Payment Schedule	(k) Cloud Controls Matrix of CSA (Cloud Security Alliance) & NIST	Our assumption is that the audit team is not expected to perform cloud configuration reviews or tool based scanning, and that the scope is limited to control design and effectiveness assessment. Please confirm if the understanding is otherwise. If not, please elaborate on the expectation and sample sizes.	<p>1) It is not required to run any tool based scanning or conduct configuration reviews through any tool. It is expected to verify the control placement & design, architecture review of cloud setup and effectiveness of implementation of controls defined in Cloud Controls Matrix of CSA (Cloud Security Alliance) & NIST CSF 2.0</p> <p>2) It is expected that NIST CSF 2.0 framework to be considered, by the selected Vendor, as a part of audit coverage.</p>
30	Page 32	Appendix E - Scope of Work and Payment Schedule	(k) Cloud Controls Matrix of CSA (Cloud Security Alliance) & NIST	Kindly elaborate on the specific NIST framework or publication that is expected to be considered as part of the audit coverage	<p>1) It is not required to run any tool based scanning or conduct configuration reviews through any tool. It is expected to verify the control placement & design, architecture review of cloud setup and effectiveness of implementation of controls defined in Cloud Controls Matrix of CSA (Cloud Security Alliance) & NIST CSF 2.0</p> <p>2) It is expected that NIST CSF 2.0 framework to be considered, by the selected Vendor, as a part of audit coverage.</p>

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
31	Page 32	Appendix E - Scope of Work and Payment Schedule	1. Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Our assumption is that out of the total 100 applications, 60 are critical and are required to be audited annually over the 3-year period. Kindly confirm if our understanding is otherwise.	60 Applications to be audited every year
32	Page 32	Appendix E - Scope of Work and Payment Schedule	1. Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.	Our assumption is that the remaining 40 applications will be distributed across two distinct audit cycles, with a portion to be audited once in 2 years, and the rest once in 3 years, depending on their criticality. Request you to share the approximate bifurcation across these two cycles to support effort estimation.	60 Applications to be audited every year
33	Page 33	Appendix E - Scope of Work and Payment Schedule	10. Audit working papers should be maintained for the respective observations for reference.	Request you to clarify whether there are any specific expectations, formats, or standards to be followed for maintaining audit working papers related to observations. Additionally, please confirm if there are any defined timelines or responsibilities for the retention and submission of these working papers	Working paper can be maintained as per Bidder standard however few base line requirement, proper walkthrough document, Data requested and received along with proper tracker, queries shared and responses, Draft report and final report, all observation related supporting separately to facilitate ease of navigating at the time of discussion

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
34	Page 33	Appendix E - Scope of Work and Payment Schedule	<p>14. If the audit process is completed but all reported observations are not closed by the auditees and/or closure responses are not received from the auditees and / or confirmatory audit could not be completed during the audit process because of any reasons, whatsoever, the auditing team shall carry out the confirmatory audit of the open observations subsequently.</p> <p>15. There are no restrictions on the total number of confirmatory audits. The confirmatory audit shall be carried out and completed within a period of 15 working days from the date of receipt of closure confirmations.</p>	It is understood that confirmatory audits will be initiated upon receipt of closure confirmations from SBI Life team/stakeholders. In the absence of such confirmations, the audit team will track the status of open observations on a quarterly basis. Kindly confirm if this approach aligns with your expectations or if an alternate tracking frequency is preferred.	Yes It aligns only instead of quarterly follow up Monthly will be better where there is no response or target closure date
35	2	Schedule of Events, Serial Number 7	Address for submission of Bids	We understand that online bid submission is not applicable for this RFP. Kindly confirm whether this understanding is correct.	Physical submission
36	12	9(iii)e	It is mandatory for all the Bidders to have class III Digital Signature Certificate (DSC) (in the name of person who will sign the Bid).	As this is a physical bid submission, please confirm whether it is mandatory for the authorized signatory to possess a Class-III Digital Signature Certificate (DSC) in a corporate capacity.	Not required for bid submission

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
37	26	Annexure B, Serial Number 6	<p>Education Qualification and Experience of a team: at least 2 resources and SME as and when required.</p> <p>Minimum 7 to 9 years of experience in BFSI domain in IS Audit including information & cyber security audit</p>	The Engagement Partner and Manager will be proposed for this engagement having more that 15 and 10 years of experience respectively, specifically in IS Audit, including Information and Cyber Security. They will be closely working with the team and supervising the engagement, reviewing all deliverables, and providing final approvals. They will be supported by a team of professionals with 3–6 years of relevant experience. Hope this is fine.	Minimum 5 years of experience is required for resources working on ground along with specified qualification.
38	27	Appendix B, Serial Number 6	Mandatory certifications: CISA/CISM/CISSP/OSCP/ OSCE (Minimum two)	Most of the IS audit professionals would posses one of these certifications (based on the competency they wish to specialize in). Hence, we are reading this requirement as minimum of two such team members possessing any of these relevant certifications mentioned under this clause.	As stated minimum two of these certification should be possessed by candidate. CISA will be preferable.
39	29	Appendix C	Technical Eligibility Criteria	Under the technical eligibility criteria, only the 80:20 evaluation ratio has been provided. For technical eligibility, kindly provide the evaluation matrix or scoring criteria or weightage.	Eligibility criteria is mentioned in RFP. Technical evaluation will be done by selection committee.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
40	32	Appendix E	Scope of Work and Payment Schedule: (f) DPDP Act 2023 and amendments, Rules issued	Kindly clarify the scope of the engagement with respect to the DPDP Act 2023. Is the bidder expected to conduct a policy and process review specifically in alignment with the Act's requirements, or should they perform a comprehensive assessment of the design and implementation of privacy controls to ensure full compliance with the DPDP Act?	Policy and process review specifically in alignment with the Act's requirements, along with this a comprehensive assessment of the design and implementation of privacy controls to ensure full compliance with the DPDP Act
41	39	Appendix J	Format for Submission of Client References	As we are bound by a Non-Disclosure Agreement (NDA) that restricts us from sharing client names and other sensitive details, we can share only the type/ sector of the organization that we worked with (for private sector organizations) though we can share the names of the PSU organizations. If necessary, we will share relevant information following discussions with the respective clients (post their approval) during the technical evaluation stage.	Post Selection
42	36	Appendix G	Contract / Service Agreement (Template)	The service agreement template attached to the RFP appears to be inaccessible or is not opening. We kindly request you to share a working version of the template to enable us to review the terms and conditions.	Will be provided

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
43	7	Disclaimer	NA	<p>On perusal of the RFP, we have observed that there is no mention of our liability under this engagement. Hence, requesting to include following clause:</p> <p>“In accordance with standard industry practice, our aggregate liability under this RFP and in connection with the services shall be for direct damages only and shall, in all circumstances and events, be limited to one time the fees paid to us under the engagement. We shall not be liable for any indirect or consequential losses.”</p>	Can be discussed at the time of contract
44	NA	General	Duration of audit	Could you kindly specify the duration, in months (per year) required to complete the audit?	Phase wise manner at least one report in the month of Sept and overall to be completed by Jan Month.
45	32	Appendix E	Scope of Work	Kindly confirm if separate compliance reports are required for each standard or regulatory requirement specified in the RFP	In same audit report you can state the compliance.
46	NA	General	Travel visit outside Mumbai	Kindly confirm if any travel is required outside Mumbai? If yes, please provide the location and number of visit required	Hyderabad Data centre and DR site only one visit is required.
47			General	Please let us know locations to be covered to	Mumbai Location- Seawoods One DR Site at Hyderabad

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
48			General	Please confirm only these reports (VAPT, Source Code Review, Configuration Review, Load and Performance Testing Reports) to be reviewed if yes, the number of reports please to be review.	VAPT, Source code and configuration review, Load and performance testing reports are only part of our one domain of cybersecurity scope is not only limited to this its beyond this refer IRDAI guidelines 2023.
49			General	Please confirm do you have dealing room to d	Will be finalised with selected bidder
50			General	IS there any specific checklist and report format already available for this scope of Audit.	checklist and format can be of Bidder baseline requirements are , in any report, overall opinion, executive summary, observations , Risk and impact, recommendation, Management response , Risk rating, basis of risk rating etc.
51			General	Please confirm Security Testing like performing VAPT, Source Code Review, Configuration Review, etc. will be out of scope.	Security Testing like performing VAPT, Source Code Review, Configuration Review need not to be conducted however end to end process needs to be reviewed whether efficient and effective.
52			General	Any possibility to get number of associated infrastructures for scope applications for this scope of Audit.	Confidential information will be disclosed at the time of audit
53			General	Please elaborate on requirement of (Information Technology Act 2000 and amendment thereof,) and (DPDP Act 2023 and amendments, Rules issued) to cover in this scope of Audit.	Policy and process review specifically in alignment with the Act's requirements, along with this a comprehensive assessment of the design and implementation of privacy controls to ensure full compliance with the DPDP Act

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
54	26	Appendix-B/ Bidder's Eligibility Criteria	Bidder should have experience of minimum _10__ years in providing the Services in field of IS Audit including Information Security audit	Request you to consider reducing the experience in the field of IS audit upto minimum 5 years	Not possible to reduce on technical parameters
55	26	Appendix-B/ Bidder's Eligibility Criteria	Education Qualification and Experience of a team: at least 2 resources and SME as and when required. • Mandatory certifications: CISA/CISM/CISSP/OSCP/ OSCE (Minimum two)	Page 32 of RFP Appendix -E/ Scope of Work (d) states that ISO 27001 framework is also to be considered for preparing an audit checklist. Accordingly, request you to also add ISO 27001 LA as one of the mandatory certification option.	For given scope CISA candidate is required, Further for ISO 27001 certification is additional as good to have.
56	35	Appendix-F/ Commercial Bid	Cost of Additional Application covered under IS Audit scope over & above 60 applications (cost per application per year).	While we understand that per unit price is to be quoted, kindly confirm whether below understanding is correct: Considering total application count is 100, max count of additional applications to be covered under IS audit scope would be 40 to be audited once in 2 years / 3 years based on criticality. If not, kindly confirm the approx. count of additional applications to be covered under IS audit scope	Yes. If out of 100 applications, 40 are critical and 60 are non critical, then 40 critical + 20 (1/3 of 60 non critical) applications will be covered every year.
57	35	Appendix-F/ Commercial Bid	The Price in the commercial bid has to be quoted inclusive of all taxes, levies and other taxes if any and also out of pocket expenses.	Excluding GST, please confirm which taxes are to be considered when quoting the price in commercial bid.	Only GST will be additional to the Audit Fee quoted

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
58	32	Appendix -E / Scope of work and Payment Schedule	<p>Firm shall provide an independent review and analysis of the organization's information security initiatives and objective assurance on Agreed Scope.</p> <p>Scope and objective of the information system (IS) audit is as per</p> <ul style="list-style-type: none"> (a) Relevant checkpoints and guidelines prescribed by IRDAI Guidelines issued on IRDAI/GA&HR/GDL/MISC/ 88/04/2023 issued on 24-April-23 and subsequent circulars / advisories, (b) SBIL internal IS Policy, Standards & Procedures, (c) SBI Life IT Policy, Standards & Procedures, (d) ISO 27001 framework, (e) Information Technology Act 2000 and amendment thereof, (f) DPDP Act 2023 and amendments, Rules issued (g) Guidelines issued by CERT-In on IT, Information & Cyber Security (h) NIST Cyber Security framework (i) COBIT (Control Objectives for Information Technology) of ISACA (j) SBI baseline technical IT security controls (k) Cloud Controls Matrix of CSA (Cloud 	<p>We understand that several activities such as VAPT, Application Security/Application Penetration Testing, Secure Code Review, Secure Configuration Review, BCP/DR,etc.may be mentioned as control requirements in the several standards, guidelines, frameworks,etc. listed in the clause from a) to l). Our understanding is that we are to review whether these activities have been performed and not to actually perform the activities. Please confirm.</p>	<p>Correct, As per scope for this activities need to assure whether process in place its effective and efficient to adhere IRDAI guidelines in this regards.</p>

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
59	26	Appendix-B (Sr No. 4)	Bidder Should be based out of Mumbai, with at least team size of 50 technically qualified person and Above. Should have qualified CISA members in their team.	Whether qualified CISA members is mandatory for this project as you have also mentioned other Certifications for auditors like CIA/CISSP/CIMS/ OSCP, Please clarify ?	Minimum two technical qualifications required and in that CISA is mandatory
60	26	Appendix-B (Sr No. 6)	Education Qualification and Experience of a team: at least 2 resources and SME as and when required.	Please clarify the total no. of Auditors required for deployment and also the deployment mode (Onsite/OFF-site & Hybrid)	Auditors are required on site Minimum 2 and 1 more SME if in case any specific matter to be checked for ex you have 2 resources working on assignment for audit of Cybersecurity if you require some one expert in VAPT and Secure code to review VAPT and secure code review report it is expected to be reviewed by subject matter expert.
61	27	Appendix-B (Sr No. 6)	Graduation in Electronics and Telecommunications or Computer Science or Information Security or Cyber Security or MCA • Mandatory certifications: CISA/CISM/CISSP/OSCP/ OSCE (Minimum two)	Please clarify Mandatory certifications requirement (Minimum 2)	1-Graduation in Electronics and Telecommunications or Computer Science or Information Security or Cyber Security or MCA. AND 2- Minimum two of the following CISA/CISM/CISSP/OSCP/OSCE
62	35	Appendix-F	Commercial Bid: The Price in the commercial bid has to be quoted inclusive of all taxes, levies and other taxes if any and also out of pocket expenses. Please note to exclude GST.	Is there any predefined budget or cost ceiling allocated for this project (ideal Bid Budget).	NA

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
63	32	Appendix-E	Scope of Work and Payment Schedule	Please clarify the detaild Scope of Work,	Scope as mentioned in the RFP and further invoices to be raised yearly in phase wise (2 or 3)post issuance of final reports, to be decided at the time of audit.
64	32	Appendix E	<p>1. Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBI Life within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality.</p> <p>2. Effectiveness of the IT Security Operations and Information Security Risk management structure and roles, evaluating adequacy of operating processes, internal controls and conducting functionality review of the above-mentioned applications.</p>	<p>Please provide us the clarification whether Application Security Review, Source Review and Network Review needs to be performed for all the application.</p> <p>We understand that security review of applications to be performed on annual basis. Please provide the count of critical application in scope.</p>	As per scope review whether these activities have been performed effectively and efficiently by reviewing reports and not to actually perform the activities ensure as per IRDAI guidelines all observations are properly closed.
65	26	Appendix B	<p>Bidder Should be based out of Mumbai, with at least team size of 50 technically qualified person and Above.</p> <p>Should have qualified CISA members in their team.</p>	Please confirm our understanding that not all 50 resource required CISA.	<p>Yes. Staff strength of the firm should be minimum 50 having various certifications and CISA is one of them.</p> <p>Resources working on assignment should be CISA.</p>

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
66	26	Appendix B	<p>1-Educational qualifications: Graduation in Electronics and Qualification and Experience details Internal</p> <p>Page 27 of 39</p> <p>Telecommunications or Computer Science or Information Security or Cyber Security or MCA</p> <ul style="list-style-type: none"> • Mandatory certifications: CISA/CISM/CISSP/OSCP/ OSCE 	Request the team to include IS Audit certification such as ISO27001:2022 in the mandatory eligibility criteria.	ISO 27001 LA can be additional qualification in addition to requirements specified in RFP.
67	27	Appendix B	<p>Education Qualification and Experience of a team: at least 2 resources and SME as and when required.</p> <p>2-Experience: Minimum 7 to 9 years of experience in BFSI domain in IS Audit including information & cyber security audit and have handled such assignments in the past for minimum 3 clients end to end from BFSI sector and subject to evaluation of proposed auditors' profile, by respective SBIL authorities during the actual assignment</p>	<p>Please confirm our understanding that 2 L2 Resources are required to perform audit.</p> <p>Also, request the team to accept minimum experience required for L2 resource should be from 5 to 9 years.</p>	Not possible to reduce on technical parameters
68	27	Appendix B	Audit team shall be dedicatedly stationed at SBIL CPC Seawoods office for the period of Audit at the expense of Service provided.	Please confirm our understanding that this is outcome based assessment and resource will not be required to be at site at the time of audit only.	Auditors are required to be onsite at SBI Life offices at Seawoods and Natraj as per requirement.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
69	17	Validity Of Contract	The Contract shall be valid for the period of one year(s) unless terminated early as per the specific contract terms.	Please provide us the confiramtion of contract period.	As mentioned in the RFP Document the duration is 3 years, the contract will be awarded on annual basis post performance evaluation.
70	26	Appendix B	Bidder Should have undertaken IS Audit of At least one PSU and Govt organization in Last 12 Months. Name and Details and Commercials of Such IS Audit	Request you to Kindly revise the criteria, as disclosing commercial information is not permitted.	Name of the client and nature of engagement to be specified.
71	32	Appendix E	Effectiveness of the IT Security Operations and Information Security Risk management structure and roles, evaluating adequacy of operating processes, internal controls and conducting functionality review of the above-mentioned applications.	Please confirm our understanding that controls will be assess and UAT will not be required.	UAT will not be required all conclusions will be based on past data to be analysed only on specific cases like system hardening actual testing is required further any checks where past data may not conclude better or it will conclude wrong observation then as on date data to be analysed.
72	2	Schedule of Events	Last date and time for Bid submission	Request you to extend the Bid submission time by one week.	Extended till 8 July 2025 till 6:25 PM

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
73	11	9	The Technical Bid and Commercial Bid are to be submitted separately in different envelopes at the address mentioned in the 'Schedule of Events'.	Please confirm if the technical and commercial proposal needs to be send physically on the shared address or sending out the proposal via mail will suffice? Address: Chief Audit Officer, SBILINSURANCE COMPANY LTD., 2 nd Floor, Natraj, M V Road and Western Express Highway Junction, Andheri (E), Mumbai – 400069. Maharashtra, India	Physical submission
74	26	Appendix B - Bidder's Eligibility Criteria (4)	Bidder Should be based out of Mumbai, with at least team size of 50 technically qualified person and Above. Should have qualified CISA members in their team.	Kindly confirm whether the resources deployed onsite will be provided with SBIL laptops and necessary access, or if the bidder is expected to provide their own hardware for the audit engagement.	Yes, SBIL will provide dedicated PC's at seawoods all workings to be carried on assigned system only, further for report preparation and review at your end vendor laptops can be used.
75	26	Appendix B - Bidder's Eligibility Criteria (8)	Start and End Date of the Project to be mentioned) in the past (At least __ client references are required)	Please confirm minimum number of client references required and can a relaxation on disclosing client name be given owing to confidentiality.	At least 5 reference (BFSI sector)

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
76	32	Appendix E- Scope of Work and Payment Schedule (1)	Audit would be conducted for 100 applications (60 applications each year) and related infrastructure components of SBIL within a span of 3 years. 100 applications include critical applications which are to be audited every year and other applications to be audited once in 2 years / 3 years based on criticality	Please confirm that the scope of the audit limits to the 100 applications & configuration of it i.e., VAPT, etc. will not be under scope.	As per the scope , review needs to be done whether VAPT, App sec testing and Secure code review activities have been performed effectively and efficiently by reviewing reports and not to actually perform the activities and to ensure that all observations are properly closed as per the IRDA guidelines.
				Kindly clarify what specific infrastructure components are included within the scope (e.g., firewalls, IDS/IPS, servers, cloud infrastructure, endpoints, etc.). Additionally, please confirm whether the audit is expected to include any physical security review of infrastructure such as data centers or server rooms.	Yes as a part of network security IT infra component are to be reviewed and physical visit at data centre and server room is required.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
				<p>1. Please clarify if the list of 100 applications along with their criticality classification will be shared with the selected bidder at the beginning of the engagement.</p> <p>2. Are mobile applications, third-party hosted systems, or cloud-native apps included in this list</p> <p>3. Kindly confirm who will determine the annual audit schedule SBIL or the selected bidder and if this will be shared at the start of each year.</p>	<p>There are 100 applications out of which 60 applications will be done annually. Further there may be additional application as the need may arise so kindly quote in two parts one for 60 applications and second part price per application.</p> <p>1- List will be shared at the beginning of the engagement.</p> <p>2-yes it will be included.</p> <p>3-Audit schedule can be discussed mutually will be shared at the beginning of the year.</p>
77	32	Appendix E- Scope of Work and Payment Schedule	The Auditing Team shall prepare an audit checklist based on above regulations, policy frameworks, guidelines, practices etc. within first month of the engagement.	Please confirm if any specific prioritization or weightage needs to be given to certain frameworks or standards over others while preparing the audit checklist.	IRDAI Regulation in consonance with NIST, ISO, COBIT

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
78	33	Appendix E- Scope of Work and Payment Schedule (11)	Audit report should contain application business process, executive summary, audit approach, audit scope, audit framework with areas/domains assessed, overall compliance status/chart, domain-wise compliance chart, risk categorization, risk scores, domain wise key risk areas, top 10 overall risks, key risk areas from SBIL side (if found), open key risk areas, key overall recommendations to be implemented by SBIL management.	Please confirm if there is a template or format for the audit report that the bidder must follow. If yes, please share a sample.	format can be of bidder baseline requirements are , in any report, overall opinion, executive summary, observations , Risk and impact, recommendation, Management response , Risk rating, basis of risk rating etc.
79	33	Appendix E- Scope of Work and Payment Schedule (13)	Management Presentation to be prepared based on the above audit report and should be presented to SBIL senior management after getting a confirmation from SBIL-Inspection & Audit team. Senior officials of the firm, having expertise in application audit should be present during the management presentation.	Please clarify the expected frequency of such management presentations (e.g., annually, per audit phase, or as required).	Audit can be conducted in phases to be decided post selection.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
80	33	Appendix E- Scope of Work and Payment Schedule (15)	There are no restrictions on the total number of confirmatory audits. The confirmatory audit shall be carried out and completed within a period of 15 working days from the date of receipt of closure confirmations.	We request SBIL to consider placing a reasonable cap on the number of confirmatory audits per application (e.g., one or two rounds) to ensure effective effort planning and avoid scope creep. Alternatively, additional rounds beyond a defined threshold may be handled on a mutually agreed basis. We also suggest implementing a batched scheduling approach (e.g., bi-weekly or monthly) for confirmatory audits to enhance operational feasibility and ensure smoother execution, particularly when multiple closure confirmations are received around the same time.	Objective of confirmatory audit is to ensure compliance and total closure. Scope details will be discussed with selected vendor.
81	33	Appendix E- Scope of Work and Payment Schedule (6)	It shall also include any other areas as may be intimated by the Company from time to time.	We acknowledge that any additional scope introduced during the engagement will have commercial implications. We request that any such scope changes be mutually agreed upon in writing before implementation, along with agreement on associated timelines and costs.	yes any scope changes and cost factors will be discussed before finalisation.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
82	36	Appendix - G (Contract / Service Agreement)	N/A	Though the RFP document refers to Contract/Service Agreement as the document to be considered as the Definitive Agreement between the parties, the same is an image format and is therefore not an accessible file. It would be viable for the same to be provided so Bidder can indicate provisions where Bidder may require to negotiate the terms of the definitive Contract once the RFP is awarded. These would be only to address very critical items (Limitation of liability, Pre-existing IP rights, etc). Request you to clarify this.	Will be provided
83	37	Appendix - H (Non-Disclosure Undertaking)	The Bidder shall indemnify SBI Life, its directors, officers, employees, subsidiaries and /or affiliates and hold them harmless against any loss or damage that SBI Life, its directors, officers, employees, subsidiaries and /or affiliates may sustain on account of any leakage of confidential information pertaining to and supplied by SBILor on account of any violation of intellectual property, confidentiality, privacy, patents, trademark etc., by the Bidder in respect of any Intellectual Property, practices, hardware, software, systems, process, technologies, etc. in whatever manner described.	There is an Indemnity provision in the Confidentiality Undertaking which we would request to delete/modify as the NDU is not a definitive agreement for services which would contain relevant provisions to address risk. In case there is breach of confidentiality or IP obligations at the bidding stage, there would always be recourse via damages or injunction through the court which would be the apt recourse. Request you to clarify if this could be accommodated?	Legal vetting at both sides would be done at the agreement stage.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
84	2	Schedule of Events	Last date for requesting clarification: 19th June 2025	Can SBIL confirm the time and platform for the virtual pre-bid meeting? Will a recording or minutes be shared post-meeting?	Details will be discussed and shared with concerned bidder.
85	27	Appendix - B - Bidder's Eligibility Criteria	The SME shall have minimum 12 to 15 years of experience in IS Audit including information & cyber security and shall utilize at least 0.25 % of efforts of combined efforts of above two-member audit team for review of (a) the entire audit process as well as confirmatory audit process, (b) Audit checklist (c) observations reported from initial audits as well as confirmatory audits and (d) Initial audit reports and confirmatory audit reports	Can SBIL confirm if the SME's 0.25% effort is calculated per audit or across the entire engagement?	It will be per audit year for this IS audit.
86	33	Appendix-E	If the audit process is completed but all reported observations are not closed by the auditees and/or closure responses are not received from the auditees and / or confirmatory audit could not be completed during the audit process because of any reasons, whatsoever, the auditing team shall carry out the confirmatory audit of the open observations subsequently.	Is there a defined process or timeline for receiving closure confirmations from auditees?	Yes all observations are to be closed before end of Financial year further open observations are highlighted to higher management.

Sl. No	RFP Page No	RFP Clause No.	Relevant extracts of respective Clause	Query/Suggestions	Response
87	35	Appendix-F	Commercial Bid	Should the commercial bid include cost for confirmatory audits separately or is it expected to be part of the overall audit cost?	Part of the overall cost
88	37	Appendix-H	Non-Disclosure Undertaking	Can the NDA be submitted on company letterhead initially and executed on stamp paper post award?	Ok
89	17	Clause 24	As per scope of this RFP, sub-contracting is not permitted. All the auditors including the SME must be on the pay rolls of the vendor. Contract resources are not permitted to do the audit, data collection , report preparation and any other audit activity.	Can SBIL clarify if third-party consultants or freelancers are allowed if they are on the payroll during the audit period?	Not allowed
90	15	Clause 18	Award Criteria	Will SBIL consider past performance and domain expertise in addition to commercial evaluation?	yes
91	30	Appendix-D	Market standing National/international reputation of the bidder (awards, certificates issued in India/abroad, scale and profitability of operations etc will be considered)	Is there a preferred format or word limit for describing market standing and reputation?	As per your convenience
92	NA	NA	General	Request to please extend Bid submission date till 2nd July 2025	Extended till 8 July 2025 till 6:25 PM
93	26	Appendix - B - Bidder's Eligibility Criteria (3)	Bidder Should be Cert-In Empaneled and its empanel should be valid during the period of Services.	Please confirm our understanding that the Bidder must possess an active CERT-IN empanelment certificate as on the date of bid submission, and that this empanelment should remain valid for the entire duration of the Services	yes Active Cert-In empanelment is mandatory