Request for Proposal (RFP)

RFP for Integrated Security Services

SBI Capital Markets Ltd

Ref: RFP no. CO/IT/2127
Date: 30-Sep-2021

Contact Details & Email id

Mr. Krishna Prajapati - Mob: +919892455267
Email - krishna.prajapati@sbicaps.com

Ms.Kalpana Shah - Mob: +919323795243
Email – kalpana.shah@sbicaps.com

We at SBI Capital Markets Ltd. (SBICAP) are pleased to invite bids from you for Integrated Security Services during the year 2021-2022 & 2022-2023. This RFP is limited to the **SBI empaneled vendors** for Information Security related services. All the terms of services including (but not limited to) SLA, NDA, etc. shall be as agreed with SBI during the empanelment process.

This RFP is not an offer by SBICAP, but an invitation to receive responses from the Bidders. No contractual obligation whatsoever shall arise from the RFP process unless and until a formal contract is signed and executed by duly authorized official(s) of SBICAP with the selected Bidder.

1. Tender Details

1.1. This tender comprises Security Assessment for SBICAP as per the specifications mentioned in technical details at Annexure – A1&A2.

1.2. The technical and commercial proposal with the relevant information/documents/acceptance of all terms and conditions as described in this RFP document will be submitted online through M/s e-Procurement Technologies Ltd., Ahmedabad, the authorized agency approved by SBICAP for e-tendering on the website https://etender.sbi/SBI/.

1.3. For any query related to e-tender and bid submission, the bidders may contact M/s e-Procurement Technologies Ltd., Ahmadabad as mentioned below:
Ravi Sheladiya
e-Procurement Technologies Limited
Email: ravi.s@auctiontiger.net
Phone: +91- 9081000428

- The Bidders will have to upload the duly signed and scanned tender documents and all Annexure Forms as part of technical bid online.
- The tender document is not required to be sent to us in hard copy.

1.4. Date Chart:

i)	Date of issue of Tender	: 30-Sep-2021
ii)	Pre-Bid queries submission	: 08-Oct-2021
iii)	Last Date of submission of Bids (online)	: 20- Oct -2021: 14:00 hrs.
iv)	Opening of Technical Bid:	: 20- Oct -2021: 14:30 hrs.
v)	Opening of Commercial Bid	: 20- Oct -2021 :17.00 hrs.

1.5. Validity of Rate Contract: 24 months from the date of Price Discovery.

1.6. It's a Closed Bid Process, the bidder is required to submit Technical & Commercial Bid on e-Tender website.

1.7. Selected vendor would be awarded the contract for supply of said services for a period of one year at the rate discovered in the tendering process.

2. Terms & Conditions

2.1. No tenders shall be accepted after the stipulated date and time.

2.2. SBICAP reserve the right to accept in part or in full or reject the entire quotation and cancel the entire tender, without assigning any reason there for at any stage.

2.3. Tender should **strictly confirm to the specifications.** Tenders **not conforming** to the specifications **will be rejected summarily.** Any incomplete or ambiguous terms/ conditions/ quotes will disqualify the offer.

2.4. Any terms and conditions from the bidders are not acceptable to the SBICAP

2.5. SBICAP reserves the right to impose and recover penalty from the vendors who violate the terms & conditions of the tender including refusal to execute the order placed on them for any reasons.

2.6. The validity period may be extended at the discretion of SBICAP which will be binding on the vendors.

2.7. Notwithstanding approximate quantity mentioned in the Tender the quantities are liable to alteration by omission, deduction or addition**.** Payment shall be regulated on the actual work done at the accepted rates and payment schedule.

2.8. The prices should be **exclusive of all taxes**, the vendor should arrange for obtaining of permits wherever applicable.

2.9. During the validity period of tender quotes, any upward change in the exchange rate/ excise duty and customs duty are to be borne by the vendor. In the event of any downward revision of levies/duties etc., the same should be passed on to SBICAP, notwithstanding what has been stated in the quotation or in the Purchase Order.

2.10. The Vendor should attach all the related product literature, data sheets, handouts, evaluation reports etc., pertaining to the Security Assessment for which the Vendor has quoted.

2.11. The Security Assessment should be started within 1 week from the date of placing the letter of Intent / Purchase order whichever is earlier. If delayed, SBICAP will charge a penalty of 1% of order value for every week of delay, subject to a maximum of 5% of the order value or will lead to cancellation of the purchase order itself.

2.12. The tools used for Security Assessment by the vendor should be licensed one.

2.13. Cloud based solution / tools and the channel being used, should be clearly stated.

2.14. It would be binding upon the vendor to maintain security and confidentiality of SBICAP systems

3. **Payment Terms**:

3.1. The payment will be made after successful completion and delivery of the acceptable Confirmatory Scan report as follows :

i. Payment shall be made in Indian Rupees.

ii. 25 % quarterly payment will be made after successful completion of the delivery of the acceptable Confirmatory Scan report for VA.

iii. 100% after successful completion of the delivery and acceptable Confirmatory Scan report for other yearly security reviews.

4. **Technical Proposal**

4.1. **Scope of Work –** Security Audits : Annexure – A1.

4.2. **Scope of Work –** Information Security Program Management : Annexure – A2

4.3. **Inventory for the scope of work** : Annexure – B.

4.4. **Technical specifications** required for the items at Annexure – C, also provides space to indicate/ record your response in an unambiguous manner through email.

4.5. To ensure uniformity at the time of evaluation and finalization of offers you should *strictly follow the format* indicated in the Annexure-E and also adhere strictly to the indicated configuration while submitting the offer.

4.6. The Technical bids will be examined by the Technical Committee of SBICAP which may call for clarifications/additional information from the bidders which must be furnished to the Technical Committee in the time stipulated by the Technical Committee.

5. **Commercial Proposal:.**

5.1. The bidder is required to submit Commercial Proposal on eTender Website in the Prescribed Format mentioned in Annexure-D1 & D2.

5.2. Prices quoted must be "All Inclusive" **except taxes as applicable**.

Annexure – A1

Scope of Work – Security Audits

Sr. No.	Details	Description	Delivery	Frequency
1	Vulnerability Assessment (Internal)	Vendor to probe Devices, Servers and applications for any possible vulnerability and attack in non-intrusive manner. Confirmatory Scan report needs to be submitted before start of next quarter.	Report of the tests and suggestions on mitigation action with proof and recommendations.	Quarterly
2	Penetration Testing (PT)	Vendor to exploit vulnerability on websites & IP Addresses provided by us and attack in non-intrusive manner. 1. Confirmatory Scan will be intimated to the vendor one week in advance.	Report of the tests and suggestions on mitigation action with proof and recommendations.	Yearly (On-Demand)
3	Secure Network Architecture Review	1. Placement & Security of servers & network devices for all integrations in SBI & SBICAP Network 2. Firewall Rule Base Review 3. Analysis of traffic monitoring (inward and outward traffic)	Report of the tests and suggestions on mitigation action with proof and recommendations.	Yearly
4	Application security review	1. AppSec of application 2. Role based Application review	Report of the tests and suggestions on mitigation action with proof and recommendations.	Yearly
5	Secure Configuration Audit	Configurations of all components such as OS, Database, Application server, web server etc. need to be reviewed (script based or manual) against SBI-SBICAP's SCD/ Benchmark	Assessment report with suggestions on improving the architecture. Point out the vulnerabilities and risks in terms of security.	Yearly

		Document.		
6	Process Review	1) Process flow including; 2) User management, privilege access etc., change control management, generation and checking of logs, incident management, flow of both to & fro traffic (its contents and the format in which it is travelling), storage at any point, password management, security environment, Compliance with SEBI guidelines and SBICAP IT Policy and IS Security Policy and industry best practices. 3) Assessment of security risk involved in data being processed/handled at third party vendor's site/location covering end to end data flow to ensure CIA of information. 4) Review of each Database on database security perspective. 5) Review of Vendor/ Third Party Access management 6) Data Flow Diagram for all the Applications to be	Assessment report with suggestions on improving the architecture. Point out the vulnerabilities and risks in terms of security.	Yearly

		obtained and 'end to end' process review, specifically on third party locations, if any need to be carried out		
7	API Review	App Security test to attempt hacking, aimed at identifying and exploiting vulnerabilities in the architecture and configuration of an API.	Assessment report with suggestions for secure configuration and find weak rules as per industry best practices.	Yearly
8	Compliance Review	As per SBI & SBICAP IT & IS Policy, Cyber Security Policy, SEBI Guidelines and Best Global Security practices		Yearly
9	BCP-DR	BCP-DR readiness as per the documented plan.		Yearly
10	Digital Forensic Readiness Assessment (DFRA)	Assessment of Forensic readiness and threat intelligence for individual Applications.		Yearly
11	Third party vendor Risk assessment	**Scope of work: -** Understand the security and compliance requirements for the Cloud applications 1. SEBI requirements 2. SBICAP policies and SBI 38 control checklist for 3rd Party. 3. Cloud security and compliance good practices 4. Review the application technical architecture from a security and compliance perspective 5. Review the agreements between SBICAP and Cloud vendors to ascertain that they meet security, compliance and legal requirements	Report of the tests and suggestions on mitigation action with proof and recommendations	Yearly (On-Demand)

Annexure – A2

Scope of Work – Information Security Program Management

The scope of work for the Information Security Program Management will be as under:

- Prepare yearly plan for all security compliance reviews / testing and all other activities related information and cyber security in the form of an **IS Program Management Calendar** and ensure execution of the activities accordingly.
- The selected ISSP shall formulate the KPIs for each of the information security activity and services, for monitoring as well as tracking. The SLA's and IS policies and procedures need to be considered while formulating the KPIs. This activity needs to be completed within initial 2 months of the engagement.
- The KPIs, defined by the ISSP shall be reviewed and have to be accepted & approved by SBICAP. The KPIs shall be associated with TATs, penalty for not adhering with TAT etc.These KPIs shall be included in the SLA, to be signed between the ISSP and SBICAP.
- Security Review / risk quantification related to niche areas such as review of new/ emerging IT initiatives in cloud / virtualisation / AI/ML/IOT, etc.
- The selected ISSP shall depute a senior consultant of L3 level having minimum 8 years of relevant technical experience as Project Manager for SBICAP for IS Program Management and managing all the activities related to Information & Cyber Security and Information Risk Management. The scope, defined for program management in this scope, is an indicative list; the selected ISSP shall follow the industry best practices for end-to-end program management / project management of all information & cyber security activities of SBICAP. Persons having industry recognized Information Security certification shall be preferred.
- The Project Manager shall visit SBICAP office at least 2 days in a week to take stock of all the activities, interact with SBICAP members and other stakeholders to ensure that all assigned/scheduled activities are completed smoothly in time.
- Review of all services, defined under the scope of this RFP, as well as IS program management activities shall be reviewed by the Project Manager of the ISSP with SBICAP CISO on weekly basis. The ISSP may deploy any project management / program management tool at SBICAP for smooth management of all activities.
- Review of all services, defined under the scope of this RFP, as well as IS program management activities shall be reviewed by Director of the selected ISSP with the CISO of SBICAP on monthly basis. Program Manager / Project Manager of the ISSP shall be present in this review meeting.
- Review of Information & Cyber Security posture of the respective SBICAP team on monthly basis with team heads of IT, HR, Management Services and other relevant business departments on pending open findings of various security testing, reviews, audits, ATRs of various management committee meetings etc.

- Improvements in the Information & Cyber Security posture of the company over a period of time or quarter-over-quarter, challenges faced by ISSP, existing information & cyber security risk of SBICAP, pending open findings & their risk to the business of SBICAP etc. shall be presented by the ISSP. In case the senior management of SBICAP proposes any other aspects to be presented to them during this quarterly meeting then the ISSP shall prepare & present accordingly.
- In case SBICAP decides presentation of existing security posture to the ISC, RMC, Board etc.then the ISSP shall prepare for it and present to the respective committee. The Partner and / or Director of the ISSP shall present. In case it is required to visit SBICAP for preparation or taking feedbacks of SBICAP senior management for these types of meetings then the ISSP shall depute its Director, overseeing the SBICAP services, to SBICAP.
- Support monitoring of all information security related activities of the company including the activities/assignments handled by the ISSP, maintaining overall data, providing snapshots, dashboards, tracking etc.
- The PM shall assist CISO in any IS related activities for SBICAP Group of companies.
- The PM shall support operational needs to the IT team by providing operational support.
- The ISSP shall be responsible for carrying out all the coordination/follow-up activities (Like, getting inventory details, identifying asset owners. UAT environment access, credentials, walkthrough etc.) with the application owner/IT team/Business owner required for completing activities in the Scope within the defined schedule as well as meeting the requirements of KPI & SLA.
- The ISSP /PM to suggest risk containment / risk mitigation controls in case some of the remediation suggested in the assessments report or IS compliance report cannot be implemented because of technical or business related reasons or application dependency. In this case, ISSP team should also facilitate and advise SBICAP on security risk management decision to avoid, transfer or accept information security risks.
- Once the requests are logged, the request needs to be allocated to respective team member of the ISSP and/or SBICAP viz. VA, Secure configuration review, PT, Appsec, vendor/cloud solution assessment, pre-engagement review of vendor/third party, review of SLA, inclusion of infosec clauses in RFI/RFP, preparation of RFP for SOC Services, etc. and then track it till closure with the respective team member of the ISSP and/or SBICAP IST. Adequate tracking / follow-up shall be done with the requester, in case of any more clarification / requirement for the infosec reviews/assessments. Sharing of Draft reports, taking feedback from the requester, arranging meeting between the requester & ISSP/CISO, sharing the final report, monitoring the TAT (Turn around Time) shall be carried out by the selected ISSP.
- The response time for all the requested activities, either through email or through the designated application, shall not exceed 24 hours. The activities requested before

1 PM shall be responded before end of the same day.

- The Program Manager shall monitor the KPI/TAT/SLA for all the activities related to Information & Cyber Security including the in-scope activities defined in this RFP as well as monitor Event/Incident triaging of New Generation SOC, scheduling of meeting between Program Manager with team heads on monthly basis and other meetings with ISSP representatives as required.
- Periodic follow ups with stakeholders for closure of open findings and getting the required data for all the information security activities.
- Preparing, maintaining tracker/dashboards of activities/projects, ATRs in Centralized IT Service desk.
- Publishing monthly dashboards / tracker for individual activities as well as consolidated monthly dashboard for all the activities to different IT and Business teams
- Follow-up and coordination with other team members to provide input in Centralized IT Service desk.
- Timely reminders / escalations for deadline to the team members for ATRs of different management meetings, tasks assigned by senior management, and other activities as scheduled in ISMS calendar, IS Program Management Calendar etc.
- Ensuring that ATRs for ISC, ISSC, ISC ATR Review Committee etc. are updated in time andtracked.
- Maintaining Files, documents, approvals, approved deviations etc. related to Information & Cyber Security.
- The tracking of approved deviations/exceptions, expiry of deviations, informing the initiator & their reporting manager on expiry of deviations, informing to technical assessment team etc. shall be carried out by the PMC
- The PM shall support the IS awareness activities, conducted by SBICAP on periodic basis, by coordinating with the end users and their team leaders, team heads etc. to ensure maximum participation in the awareness activities.
- Assess, Develop and Review Information Security Performance dashboards focused on various measures such as effectiveness on the various services under ISS based on the KPI measurement.

Deliverables - Dashboards, MIS, Tracking, Presentations, MOM, KPIs, etc.. Any other services - SBICAP may from time to time, seek additional services from the service provider as it may deem appropriate. The services will be adhoc in nature and the service provider will have to make resource available as and when requested for by SBICAP.

Annexure – B

Security Assessment Inventory

Sr. No.	Security Review	Details	Frequency	BOQ
1	Vulnerability Assessment	Servers+NW devices	4	42
2	Penetration Testing	Ext. IPs/URLs	1	10
3	Secure Network Architecture Review (Incl. FAR, WiFi Rules, SaaS connectivity, etc.)	Project	1	1
4	Application Security Review			
4.1	No. of pages / App1	11000	1	1
4.2	No. of pages / App2	Around Dynamic/Static Pages	1	1
4.3	No. of pages / App3	12 static	1	1
4.4	App4	100 static	1	1
4.5	App5	40 dynamic	1	1
4.6	App6	40 dynamic	1	1
4.7	App7		1	1
4.8	App8		1	1
4.9	App9		1	1
5	Secure Configuration Audit	Project	1	30
6	Process Review	Project	1	1
7	API Review	Project	1	1
8	Compliance Review	Project	1	1
9	BCP-DR	Project	1	1
10	Digital Forensic Readiness Assessment (DFRA)	Project	1	1
11	Third party vendor Risk assessment	Project	1	1

Annexure – C

Technical Bid Specifications (To Be submitted on Email)

Technical Evaluation Parameters	**Name of Tool used**	**Is the tool Licensed Yes/No**	**Test will be done On-site / Off-site / Cloud**	**Mandays reqd for L1 resource**	**Mandays reqd for L2 resource**	**Mandays reqd for L3 resource**	**Report submission days after scan**	**Compliance with tender notice Yes / No**
Vulnerability Assessment Servers								
Vulnerability Assessment Network Devices								
External PT								
Network Architecture Review								
Firewall Config & Rule Set Review								
Application Security (Appsec)								
SCD Review								
Process Review								
API Review								
Compliance Review								
BCP-DR								
Vendor Risk assessment & 38 Control checklist review								

Annexure – D-1

Commercial BID
Prices excluding taxes

Sr. No.	Security Review	Details	Frequency	BOQ	Unit Price Rs.	Total Price (Rs.)
1	Vulnerability Assessment	Servers+NW devices	4	42		
2	Penetration Testing	Ext. IPs/URLs	1	10		
3	Secure Network Architecture Review (Incl. FAR, WiFi Rules, SaaS connectivity, etc.)	Project	1	1		
4	Application Security Review					
4.1	No. of pages / App1	11000	1	1		
4.2	No. of pages / App2	Around Dynamic/Static Pages	1	1		
4.3	No. of pages / App3	12 static	1	1		
4.4	App4	100 static	1	1		
4.5	App5	40 dynamic	1	1		
4.6	App6	40 dynamic	1	1		
4.7	App7		1	1		
4.8	App8		1	1		
4.9	App9		1	1		
5	Secure Configuration Audit	Project	1	30		
6	Process Review	Project	1	1		
7	API Review	Project	1	1		
8	Compliance Review	Project	1	1		
9	BCP-DR	Project	1	1		
10	Digital Forensic Readiness Assessment (DFRA)	Project	1	1		
11	Third party vendor Risk assessment	Project	1	1		

Annexure – D-2

Rate Contract:

SBICAP shall have a rate contract with the ISSPs for carrying out any activity related to information and cyber security services, BCP/DR services, Data governance services, Forensic services, ISO 2000 services, Product evaluation, security solution consulting, IT governance services etc. as per scope mentioned in Annexure – A2. So, the bidders are requested to provide below rates.

S No	Resource Level	Resource Cost per person /per day (Rs.)	Resource Cost per person / per month (Rs.) (if retained for a minimum duration of one month for a regular routine)
1	L-1		
2	L-2		
3	L-3		
4	L-4		

Commercial quotes of Bidders will be opened, evaluated and the rates will be normalized for each level.

Post rate contract, the allocation / distribution of activities / assignments will be solely at the discretion of the SBICAP, which may include calling RFP/RFQ for getting effort estimates.

Rate Contract by SBICAP does not confer any right on the ISSP to receive assignments / activities / work orders.

The SBICAP reserves the right to accept the bids or opt for negotiation and offer the rates or cancel this part of the RFP process.

Yearly step up at 6%

Outstation Travel – Out of Pocket / Lodging /Boarding expenses – on actuals subject to a maximum of Rs. 4000 /-per day for metro and state capitals and Rs.2,500/- per for other locations.

Air Travel – Economy class lowest fare from

Company's head office / Mumbai/current location of resource whichever is lowest to the activity location

Note: The quoted prices shall be exclusive of all taxes and statutory levies such as Service Tax/VAT, Sales Tax etc. All taxes & statutory levies should be specified explicitly.

Annexure - E

Bidders Profile

Sr. No.	Documents	Attached in bid (Yes/No)
1.	Complete tender document containing duly filled in, signed with company seal, wherever required.	
2.	Years of Experience in Security Audit	
3	Employee Strength	
4.	Turn Over details for last three years with Profitability	
5.	Qualification and Experience of Resources assigned for this project	
6.	Present Clients engagement in BFSI	
7.	Certification Standards Achieved	
8.	Any other relevant documents	

Request for Proposal (RFP)
RFP for Integrated Security Services

SBI Capital Markets Ltd
Ref: RFP no. CO/IT/2127
Date: 30-Sep-2021

Corrigendum & Addendum No. 1 dated 06th October 2021

Contact Details & Email id

Mr. Krishna Prajapati - Mob: +919892455267
Email - krishna.prajapati@sbicaps.com

Ms.Kalpana Shah - Mob: +919323795243
Email – kalpana.shah@sbicaps.com

Tentative Factsheet for Tender Submission

Date of issue of Tender	30-Sep-2021
Pre-Bid queries submission	08-Oct-2021
Last Date of submission of Bids (online)	Previous Date: 20- Oct -2021: 14:00 hrs Change Date: 18- Oct -2021: 12:00 noon hrs
Opening of Technical Bid:	Previous Date: 20- Oct -2021: 14:30 hrs Change Date: 18- Oct -2021: 12:15 hrs
Opening of Commercial Bid	Previous Date: 20- Oct -2021 :17.00 hrs Change Date: 18- Oct -2021 :13.00 hrs