Queries submitted against RFP for Supply, Installation, Configuration, Integration, Testing, Training, Commissioning, Operations & Maintenance (Three Years) of CYBER RANGE Platform for Rajasthan Cyber Security CoE (NIB no. F3.3(449)/RISL/Tech/Misc/2022/8280 Dated: 02.03.2023.)

S.No.	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Response by RISL
1	8	2.PRE-QUALIFICATION/ ELIGIBILITY CRITERIA FOR BIDDER	Sr.no- 4 (Technical Capability) The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC) OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 6 Crores each.	We may request you to modify the clause as below : The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC) OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within five years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 6 Crores each.	Please refer to updated clause in Final RFP document.
	8	2.PRE-QUALIFICATION/ ELIGIBILITY CRITERIA FOR BIDDER	Sr.no- 2 Financial: Turnover Average Annual Turnover of the bidder from IT/ITeS during the Financial years 2018-19, 2019-20, 2020-21 (as per the audited balance sheets), should be at least Rs. 50 Crores.	Considering the size and scale of the project, we believe that a firm proven track records of delivering similar engagemnet will be the best fit for the requirement. As such we request to modify the clasue as under: Average Annual Turnover of the bidder from IT/ITeS during the Financial years 2018-19, 2019-20, 2020-21 (as per the audited balance sheets), should be at least Rs. 100 Crores.	As per RFP.
	8	2.PRE-QUALIFICATION/ ELIGIBILITY CRITERIA FOR BIDDER	Sr.no- 5 Certifications The bidder must possess at the time of bidding, a valid and latest standard/version of: - a. ISO 9001 Certification b. ISO 20000 Certification c. ISO 27001 Certification	We may request you to modify the clause as below : The bidder must possess at the time of bidding, a valid and latest standard/version of: - a. ISO 9001 Certification b. ISO 20000 Certification/ ISO 27001 Certification	Please refer to updated clause in Final RFP document.
	9	3. SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES	a) Scope of Work (SoW) Details (2.i) Supply, Install, Configure, Customise, Integrate, Test, provide Training and Commission the overall platform at RSDC, Jhalana Dungri, Jaipur, Rajasthan. Required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC).	We beileve that, required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC) or the bidder. Please clarify the same.	Please refer to updated clause in Final RFP document.
	9	3. SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES	a) Scope of Work (SoW) Details (2.iii) Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement.	This statement is vague and may not aid in the finalisation of solutions, including hardware; therefore, we may request a list of items required for integration.	Please refer to updated clause in Final RFP document.

9	3. SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES	a) Scope of Work (SoW) Details (3.ii) Deployment of skilled technical manpower as per qualifications and experience mentioned in Annexure-16 of this bidding document and ensure their availability on all working days of state government. However, if required by the Purchaser, under exceptional circumstances, ensure the availability of deployed manpower on Holidays too and without any additional financial implication to the purchaser.	We understand that an emergency can happen with any manpower, and he may require time off to fix that. In the RFP document, no such provision is available; hence, we may request to allow at least 12 calendar days of leave to deployed manpower without any penalty.	Please refer to updated clause in Final RFP document.
11	3) Project Deliverables, Milestones & Time Schedule	b) Milestones, Timelines & Deliverables Successful completion of Phase-1 as per Section 4-a-2 above.(T+8 Weeks)	As per the current industry standards, OEMs typically take 8–10 weeks to deliver hardware. So looking in the same, we may request you to kindly revise the timelines as below: (T+12 Weeks)	Please refer to updated clause in Final RFP document.
19	26) Performance Security	26) Performance Security b) The amount of performance security shall be 5%, or as may be specified in the bidding document, of the amount of supply order in case of procurement of goods and services.	We believe that the amount of performance security shall be 5% is on higher side in view of procurement cost and other tender documents of department for similar kind of work, where the amount of performance security shall be kept as 2.5%. hence; we request you to please modify the clause as: The amount of performance security shall be 2.5%, or as may be specified in the bidding document, of the amount of supply order in case of procurement of goods and services.	Please refer to updated clause in Final RFP document.
31	27) Execution of agreement	Sr. No (b) b) The successful bidder shall sign the procurement contract within 15 days from the date on which the letter of acceptance or letter of intent is dispatched to the successful bidder..	We request you to provide us at least 30 days of time for signing the contract as we will have to initiate our internal process of required approvals after getting the Letter of acceptance which may take time. Hence we request you to modify the clause as "The successful bidder shall sign the procurement contract within 30 days from the date on which the letter of acceptance or letter of intent is dispatched to the successful bidder."	As per RFP.
20	28) Confidentiality	28) Confidentiality	We would like to request you to please include the following point in this clause: The confidentiality obligations should be applicable up to one(1) year of completion of respective assignment under this empanelment.	As per RFP.

34	34) Termination	c) Termination for Convenience	We believe termination for Convenience should also be allowed for the selected agency as there may be circumstances where it may not be able to continue providing services due to conflict of interest or any other valid reason. Hence we request you to add the following clause " Either of the parties may terminate the Contract without cause by giving the other party a prior written notice of at least 1 (one) month. If either of them are in breach of this Contract and do not remedy the breach within 1 (one) month of receiving the other party's written notice specifying the breach, then the other party may terminate this Contract by giving the party in breach a written notice of 7 days. In addition, the selected agency may terminate this Contract by a written notice to the purchaser if it determine that a law, regulation or anything having a similar import, or a circumstance (including cases where your ownership or constitution has changed), makes its performance of the Contract impermissible or in conflict with independence or professional rules applicable to us. Upon termination, the purchaser agree to pay for all Services performed up to the effective date of termination."	As per RFP.
38	6. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	7. 2 (A) Performance based Service Level - Target Milestone: Successful commissioning of overall Cyber Range Platform (as per Scope of Work detailed in Section 4-a-2 of Chapter-4 of this bidding document) Payment to be Released- 76% of the quoted CAPEX after deducting Liquidated Damages, if any	We understand that OEMs charge upfront payment at the time of material delivery, which may be a huge investment for suppliers (SI). As a result, I request that you change the clause to "- 100% of the quoted CAPEX after deducting liquidated damages, if any, on successfully commissioning items or solutions.	Please refer to updated clause in Final RFP document.
64	ANNEXURE-16: MINIMUM QUALIFICATION AND EXPIERENCE OF PROPOSED TECHNICAL MANPOWER	Sr. Platform Engineer/ Administrator Masters (M.Sc./ MCA/ M.Tech.) Degree in Computer Science/ Information Technology/ Cyber Security AND Any valid certification from the list below: - a) Certified Information System Security Professional (CISSP) b) Certified Information System Auditor (CISA) c) Certified Information Systems Manager (CISM) d) Offensive Security Certified Professional (OSCP) from offensive-security e) Certified Ethical Hacker (CEH) f) any other security related certification from respective body AND At least 5 Years of Working Experience in the Cyber Security/ IT Security Domain AND Hands-on working experience on proposed platform AND Fluency in written and verbal Hindi & English Language	We request you to modify the clause as"- B.E. /B.Tech /MCA/Master's in computer or IT/ Cyber security AND Any valid certification from the list below: - a) Certified Information System Security Professional (CISSP) b) Certified Information System Auditor (CISA) c) Certified Information Systems Manager (CISM) d) Offensive Security Certified Professional (OSCP) from offensive-security e) Certified Ethical Hacker (CEH) f) any other security related certification from respective body AND At least 5 Years of Working Experience in the Cyber Security/ IT Security Domain AND Hands-on working experience on proposed platform AND Fluency in written and verbal Hindi & English Language	Please refer to updated clause in Final RFP document.

	41	ANNEXURE-2: TECHNICAL SPECIFICATIONS	S.no- 1 (b) At the time of bidding, OEM must have: - i. A valid ISO 9001, ISO 20000 and ISO 27001 certification v. Full-time Cyber Security Researchers (at least 50) vi. At least one successful deployment (proposed platform) in India in last Five years (from the start date of bidding).	We would request to modify the clause as below: At the time of bidding, OEM/bidder must have: - i. A valid ISO 9001, ISO 20000/ISO 27001 certification v. Full-time Cyber Security Researchers (at least 25) vi. At least one successful deployment (proposed platform) across globe in last Five years (from the start date of bidding).	Please refer to updated clause in Final RFP document.
2	2	Contract/ Project Period	The Contract/ Project Period shall commence from the date of issue of Work order till 5 Years of Operations & Maintenance Services after commissioning of the project.	From the scope of work details we understand the Operations & Maintenance period is for 3 years. Kindly confirm and amend the clause accordingly.	Please refer to updated clause in Final RFP document.
	10	3) a) Phase-2: Operate and Maintain (O&M) Cyber Range Platform (Three Years) i.	Operations & Maintenance of the deployed platform would be required for an initial period of Three years from the date of commissioning (Go-Live) and if required, could be extended for another period of Two years on mutual acceptance and as per rates mentioned in RISL's work order issued earlier to the successful bidder.	Request you to kindly amend the clause as follows. Operations & Maintenance of the deployed platform would be required for an initial period of Three years from the date of commissioning (Go-Live) and if required, could be extended for another period of Two years on mutual acceptance and ~~as per rates mentioned in RISL's work order issued earlier to the successful bidder~~ as per rates agreed upon by RISL and service partner.	Please refer to updated clause in Final RFP document.
	10	3) b) Milestones, Timelines & Deliverables	<table><tr><th>SNo.</th><th>Milestone</th><th>Timeline</th><th>Deliverable</th></tr><tr><td>1.</td><td>Successful completion of Phase-1 as per Section 4-a-2 above.</td><td>T+8 Weeks</td><td>• OEM(s) License & Support Certificates/ Letters/ Undertakings</td></tr></table>	The timelines of 8 weeks is very stringent to complete the procurement, functional testing, integration testing and UAT of the overall platform. Request to increase the timeline for successful completion of phase 1 to T+20 weeks	Please refer to updated clause in Final RFP document.
	13	7) Alternative/ Multiple Bids	Alternative/ Multiple Bids shall not be considered at all. Also, the bidder shall not quote for multiple brands/ make/ models of hardware but only one in the technical Bid and should also mention the details of the quoted make/ model in the "Annexure-10: Components Offered"	The clause will be limiting the SI with a single OEM .Hence request you to allow bidder to quote without any restriction on the OEMs which will help achieve a better cost optimized solution and will keep the options open post award of contract for approval and finalization.	Please refer to updated clause in Final RFP document.
	16	c) Technical Evaluation Criteria	If required, Technical presentation and/or POC may be conducted to understand the solution quoted by participating bidder. After evaluating the presentation and/or POC, the committee of experts will evaluate the technical responsiveness for each bid and decision of committee shall be binding on all the bidders.	Kindly confirm if POC or technical presentation will be required as a part of technical evaluation.	Please refer to updated clause in Final RFP document.
	19	25) Right to vary quantity	b) Repeat orders for extra items or additional quantities may be placed on the rates and conditions given in the contract. Delivery or completion period may also be proportionately increased. The limits of repeat order shall be as under: - 1) 50% of the quantity of the individual items and 50% of the value of original contract in case of works; and 2) 50% of the value of goods or services of the original contract.	The provision of right to vary quantity to 50% of the individual items or 50% of the contract is very high considering exchange rate variation, commodity price variation and bid validity. Hence as per standard practice request you to lower the limit from 50% to 5% and amend the clause as follows: The limits of repeat order shall be as under: - 1) ~~50%~~ 5% of the quantity of the individual items and ~~50%~~ 5% of the value of original contract in case of works; and 2) ~~50%~~ 5% of the value of goods or services of the original contract.	As per RFP.

26	4) Joint Venture, Consortium or Association	Unless otherwise specified in the special conditions of the contract, if the Supplier/ Bidder is a joint venture, consortium, or association, all of the parties shall be jointly and severally liable to the Purchaser for the fulfilment of the provisions of the contract and shall designate one party to act as a leader with authority to bind the joint venture, consortium, or association	Kindly confirm if JV/Consortium is allowed or not. If allowed kindly confirm the maximum number of members allowed.	Please refer to updated clause in Final RFP document.
32	27) Extension in Delivery Period and Liquidated Damages (LD) d)	ii. The maximum amount of liquidated damages shall be 10%.	We understand the maximum LD limit of 10% is on the CAPEX value. Kindly confirm	Please refer to updated clause in Final RFP document.
32	29) Warranty	The bidder must supply all items(hardware as well as software) with comprehensive on-site OEM warranty valid for five years after the goods, or any portion thereof as the case may be, have been delivered to, installed and accepted at the final destination(s) indicated in the bidding document. However, if delay of installation is more than a month's time due to the reasons ascribed to the bidder, the warranty shall start from the date of last successful installation of the items covered under the PO.	From MANUFACTURER'S AUTHORIZATION FORM (MAF) we understand the comprehensive on-site warranty is for 3 years. Kindly confirm and amend the clause accordingly.	Please refer to updated clause in Final RFP document.
34	34) c) Termination for Convenience	RISL, by a written notice of at least 30 days sent to the supplier/ selected bidder, may terminate the Contract, in whole or in part, at any time for its convenience. The Notice of termination shall specify that termination is for the Purchaser's convenience, the extent to which performance of the supplier/ selected bidder under the Contract is terminated, and the date upon which such termination becomes effective.	Termination for Convenience clause is one-sided and hence request to amend clause to extend the right to either party as follows: RISL/SI, by a written notice of at least 30 days ~~sent to the supplier/ selected bidder~~, may terminate the Contract, in whole or in part, at any time for its convenience. The Notice of termination shall specify that termination is for the Purchaser's or SI convenience, the extent to which performance ~~of the supplier/ selected bidder~~ under the Contract is terminated, and the date upon which such termination becomes effective.	As per RFP.
38	1) Payment Terms and Schedule	<table><tr><th>S.No.</th><th>Target Milestone</th><th>Payment to be Released</th></tr><tr><td>1</td><td>Successful commissioning of overall Cyber Range Platform (as per Scope of Work detailed in Section 4-a-2 of Chapter-4 of this bidding document)</td><td>76% of the quoted CAPEX after deducting Liquidated Damages, if any.</td></tr><tr><td>2</td><td>Operations & Maintenance of overall Platform (as per Scope of Work detailed in Section 4-a-3 of Chapter-4 of this bidding document)</td><td>24% of the remaining CAPEX in 12 quarterly equated installments + 100% of the quoted OPEX in 12 quarterly equated installments after deducting penalty as per SLA Clause 2(d) and 2(e) below.</td></tr></table>	Withholding 24% of the Capex for opex portion will be severely impacting the cashflow negatively. SI will already be submitting a PBG along with manpower to maintain the SLAs. There will be impact of GST also for withholding the payment of the supply items. Hence request you to kindly amend clause for payment in their corresponding Phases as follows: Phase-1 : ~~76%~~ 100% of the quoted CAPEX after deducting Liquidated Damages, if any Phase-2 : ~~24% of the remaining CAPEX in 12 quarterly equated installments +~~ 100% of the quoted OPEX in 12 quarterly equated installments after deducting penalty as per SLA Clause 2(d) and 2(e) below.	Please refer to updated clause in Final RFP document.

38	1) Payment Terms and Schedule	<table><tr><th>Proposed Major Milestone</th><th>Payments to be released</th></tr><tr><td>Kick off meeting 1. Presentation of overall timelines for execution of the project. 2. Number of team members to be deployed at site alongwith their names and escalation matrix.</td><td>10% of the Capex as interest free mobilization advance</td></tr><tr><td>Supply of the proposed platform (Cyber Range Platform & associated H/w and S/w components)</td><td>70% of the Capex on pro rata basis after deducting Liquidated Damages, if any.</td></tr><tr><td>Installation & Configuration Document duly signed + Stamped by designated team of RISL/ DoIT&C officials UAT Report duly signed + stamped by designated team of RISL/ DoIT&C officials</td><td>20% of the Capex on pro rata basis after deducting Liquidated Damages, if any.</td></tr><tr><td>Operations & Maintenance of overall Platform (as per Scope of Work detailed in Section 4-a-3 of Chapter-4 of this bidding document)</td><td>~~24% of the remaining CAPEX in 12 quarterly equated installments +~~ 100% of the quoted OPEX in 12 quarterly equated installments after deducting penalty as per SLA Clause 2(d) and 2(e) below.</td></tr></table>	As per the payment terms the complete Phase-1 is a single milestone which in turn is again impacting the project cash flow. Hence request you to kindly amend the project milestones and accordingly the payment terms in following parts:	Please refer to updated clause in Final RFP document.
38	Platform Uptime Service Levels	Penalty (in case of nonconformity to desired Service Levels in any Quarter)	There is no cap/limit on the maximum amount of SLA penalties. Hence request you to kindly add the clause to limit the maximum penalty to 10% of the OPEX amount.	Please refer to updated clause in Final RFP document.
38	e) Manpower Availability Service Levels	Non-availability on deployed/ required technical manpower	We understand that the penalty for non-availability of on-site technical manpower is excluding the sanctioned yearly paid leave. Kindly confirm	Please refer to updated clause in Final RFP document.
51	ANNEXURE-9: UNDERTAKING ON AUTHENTICITY OF COMPUTER EQUIPMENTS	In case, we are found not complying with above at the time of delivery or during installation, for the equipment already billed, we agree to take back the equipment already supplied at our cost and return any amount paid to us by you in this regard and that you will have the right to forfeit our Bid Security/ SD/ PSD for this bid or debar/ black list us or take suitable action against us.	Request you to remove the debar/blacklist option as for large conglomerate its a No-Go clause. Kindly amend the clause as follows. In case, we are found not complying with above at the time of delivery or during installation, for the equipment already billed, we agree to take back the equipment already supplied at our cost and return any amount paid to us by you in this regard and that you will have the right to forfeit our Bid Security/ SD/ PSD for this bid ~~or debar/ black list us~~ or take suitable action against us.	Please refer to updated clause in Final RFP document.
41	ANNEXURE-2: TECHNICAL SPECIFICATIONS	2. c) Note: - Bidder must ensure that the deployment, configuration, customization, integration, testing, training and commissioning of platform is done on-site by respective OEM only. Hence, required professional services of respective OEM must be accounted for in the proposal.	Requesting to modify the clause as below. c) Note: - Bidder must ensure that the deployment, configuration, customization, integration, testing, training and commissioning of platform is done on-site by respective OEM or Implementation partner only. Hence, required professional services of respective OEM or Implementation partner must be accounted for in the proposal.	As per RFP.
42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	5. l) Of 11 concurrent Users/ Tenants/ PODs, 10 should be based on open-source versions while 1 with OEM specific version (preferably OEM's academic version, if any) for which RISL share separately provide the list of existing OEMs (whose products are installed in RSDC/ RSOC) to the prospective OEMs/ Bidders (on request from the date of NIB and before the last date of bidding).	Requesting to modify the clause as below. l) Of 11 concurrent Users/ Tenants/ PODs, 6 should be based on open-source versions while 5 with OEM specific version (preferably OEM's academic version, if any) for which RISL share separately provide the list of existing OEMs (whose products are installed in RSDC/ RSOC) to the prospective OEMs/ Bidders (on request from the date of NIB and before the last date of bidding).	Please refer to updated clause in Final RFP document.

42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	6. b) It must provide isolation from the Internet and must be able to function in an air-gap environment.	Requesting to remove this clause, as it is mentioned for creating an environment with open source products as well in point 5-K in the same page.	As per RFP.
43	ANNEXURE-2: TECHNICAL SPECIFICATIONS	7. a) The platform must include a appliance based traffic generator/ simulator which is capable of simulating at least 50,000 attacks with the ability to constantly apply regular updates and additions to the list of attacks.	Requesting to modify the clause as below to open this for multiple OEMs. a) The platform must include a appliance or software based traffic generator/ simulator which is capable of simulating large number of traffic or malicious traffic with the ability to constantly apply regular updates and additions to the list of attacks.	As per RFP.
9	3. SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES a) Scope of Work (SoW) Details	iii. Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement.	Kindly clarify whether the integration is for the cyber range platform with existing production infrastructure. As per best practice, integration of cyber range platform with production infrastructure is not advisable so requesting to reconsider this integration point.	Please refer to updated clause in Final RFP document.
42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	5. j) It must include both logical and physical network components (virtualized/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorization Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	It must include both logical OR physical network components (virtualized/physical), wherever applicable and relevant to the attack scenario, including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorization Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	Please refer to updated clause in Final RFP document.
41	ANNEXURE-2: TECHNICAL SPECIFICATIONS	5. a) It must include all the essential pre-packaged scenarios (at least 50, categorized by type and complexities and searchable too) along with varying difficulty levels and step-by-step documentation/ guide with visual representation of corresponding layer for each scenario so as to facilitate a variety of real-world simple-medium-complex exercises in an isolated and sandboxed environment. Also, looking to rapidly changing Cyber Security Threat landscape, it is must that new pre-packaged scenarios, as per prevailing threat landscape, be updated by respective OEMs throughout the project duration.	It must include all the essential pre-packaged scenarios (at least 30, categorized by type and complexities and searchable too, mapped according to MITRE ATTACK framework) along with varying difficulty levels and step-by-step documentation/ guide with visual representation of corresponding layer for each scenario so as to facilitate a variety of real-world simple-medium-complex exercises in an isolated and sandboxed environment. Also, looking to rapidly changing Cyber Security Threat landscape, it is must that new pre-packaged scenarios, as per prevailing threat landscape, be updated by respective OEMs throughout the project duration.	Please refer to updated clause in Final RFP document.

	9	3. SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES a) Scope of Work (SoW) Details	iii. Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement.	Please provide the list of RISL existing tools for reference. The network shall allow integration of RISL tools as possible.	Please refer to updated clause in Final RFP document.
	54	Indicative Financial Bid Format	* GST shall be paid on actuals as per prevailing rates	We understand any statutory variation or change in law is covered. Kindly confirm	As per RFP.
3	8	4. Technical Capability	The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC) OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 6 Crores each.	Kindly clarify complete Project value will be considered or only Security solutions value will be considered for evaluation.	Please refer to updated clause in Final RFP document.
	9	a) Scope of Work (SoW) Details	Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement.	As per respective RFP clauses it has been asked to build a cyber range platform as per NIST's NICE framework by incorporating/replicating existing security layers running in existing datacenter /SOC environment including NIPS, HIPS, Anti APT, endpoint security to achieve traffic generation and threat emulation scenarios.	Please refer to updated clause in Final RFP document.
	10	3) Phase-2: Operate and Maintain (O&M) Cyber Range Platform (Three Years)	v. To ensure the timely updation/upgradation of the overall platform and associated components as and when released by respective OEM(s) with prior approval from RISL/ DoIT&C. vi. Integrations with existing and new appliances deployed in RSDC & RSOC throughout the project duration as per purchaser's and/ or platform requirement.		
	41	ANNEXURE-2: TECHNICAL SPECIFICATIONS	a) The proposed platform (Cyber Range Platform & associated H/w and S/w components) must be a purpose-built COTS product offering from a reputed OEM dealing in Cyber Security products and services. a) All the essential H/w & S/w components required to use the platform to its full capabilities must be included in the offering.		

	42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	j) It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc. k) For creating a heterogeneous environment, at least two different products (one open-source + one OEM specific) for each of the above category should be included in offering.	Please help for providing complete details on eixtsing security products with their make & model so that bidders can incorporate existing security components running in SDC/SOC environment of respective OEMs to build cyber range platform as a part of solution offering.	
4	8	2. Pre qualification criteria for bidder	The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC) OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 6 Crores each.	The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC)/ Cyber Security appliances OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within FIVE years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 6 Crores each.	Please refer to updated clause in Final RFP document.
	10	3. SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES	b) Milestones, Timelines & Deliverables Milestone: Successful completion of Phase-1 as per Section 4-a-2 above- T+8 Weeks	Please extend the timelines of Phase 1 for atleast T+15 weeks to rule out all possibilities of dealy of supplies, hardware if any need to be supply and deploy by bidder as part of its solution	Please refer to updated clause in Final RFP document.

19	Section 4, ITB, 26 Performance Security	PBG a) Prior to execution of agreement, Performance security shall be solicited from all successful bidders except the departments of the State Government and undertakings, corporations, autonomous bodies, registered societies, co-operative societies which are owned or controlled or managed by the State Government and undertakings of the Central Government. However, a performance security declaration shall be taken from them. The State Government may relax the provision of performance security in particular procurement or any class of procurement. b) The amount of performance security shall be 5%, or as may be specified in the bidding document, of the amount of supply order in case of procurement of goods and services. In case of Small Scale Industries (SSI) of Rajasthan, it shall be 1% of the amount of quantity ordered for supply of goods and in case of sick industries, other than SSI, whose cases are pending before the Board of Industrial and Financial Reconstruction (BIFR), it shall be 2% of the amount of supply order	PBG a) Prior to execution of agreement, Performance security shall be solicited from all successful bidders except the departments of the State Government and undertakings, corporations, autonomous bodies, registered societies, co-operative societies which are owned or controlled or managed by the State Government and undertakings of the Central Government. However, a performance security declaration shall be taken from them. The State Government may relax the provision of performance security in particular procurement or any class of procurement. b) The amount of performance security shall be 2.5%, or as may be specified in the bidding document, of the amount of supply order in case of procurement of goods and services. In case of Small Scale Industries (SSI) of Rajasthan, it shall be 1% of the amount of quantity ordered for supply of goods and in case of sick industries, other than SSI, whose cases are pending before the Board of Industrial and Financial Reconstruction (BIFR), it shall be 2% of the amount of supply order	Please refer to updated clause in Final RFP document.
38	Section 6, Special terms and conditions of the tender & contract	Payment Term Target Milestone: (1) Successful commissioning of overall Cyber Range Platform (as per Scope of Work detailed in Section 4-a-2 of Chapter-4 of this bidding document)- 76% of the quoted CAPEX after deducting Liquidated Damages, if any. (2) Operations & Maintenance of overall Platform (as per Scope of Work detailed in Section 4-a-3 of Chapter-4 of this bidding document)- 24% of the remaining CAPEX in 12 quarterly equated installments + 100% of the quoted OPEX in 12 quarterly equated installments after deducting penalty as per SLA Clause 2(d) and 2(e) below.	OEMs has no policy to customer linked payments and realize their 100% payment within 1-2-or 3 months of time period. The solution requirement of RISL also indicating supplies for meeting the prupose of use cases, other than Cyber range as well. We therefore requesting you to not linked the entire payment of bidder for the supplies that are not linked with Cyber range platform. We suggest to propose the following payment terms for your conisderation: (1) Successful commissioning of overall Cyber Range Platform (as per Scope of Work detailed in Section 4-a-2 of Chapter-4 of this bidding document)- 90% of the quoted CAPEX after deducting Liquidated Damages, if any (2) Operations & Maintenance of overall Platform (as per Scope of Work detailed in Section 4-a-3 of Chapter-4 of this bidding document)- 10% of the remaining CAPEX in 12 quarterly equated installments + 100% of the quoted OPEX in 12 quarterly equated installments after deducting penalty as per SLA Clause 2(d) and 2(e) below.	Please refer to updated clause in Final RFP document.
26	5. General terms & conditions of the tender & contract	4) Joint Venture, Consortium or Association	Please clarify whether consortium is allowed in the Project or not, as nowhere in RFP it is denied. If consortium is allowed, what are the eligibility conditions for the consortium partner, it cannot be less than what expirence has been asked from bidder.	Please refer to updated clause in Final RFP document.

Page 32	ANNEXURE-2: TECHNICAL SPECIFICATIONS	29. Warranty The bidder must supply all items(hardware as well as software) with comprehensive on-site OEM warranty valid for five years after the goods, or any portion thereof as the case may be, have been delivered to, installed and accepted at the final destination(s) indicated in the bidding document.	The Project is of 3 years, please consider to correct it as 3 years.	Please refer to updated clause in Final RFP document.
Page 41	ANNEXURE-2: TECHNICAL SPECIFICATIONS	b) At the time of bidding, OEM must have: - i. A valid ISO 9001, ISO 20000 and ISO 27001 certification	We kindly suggest that OEM should have one of the provided ISO certifcations only, moreover OEM being into security domain ISO 27001 is more relevant to ask.	Please refer to updated clause in Final RFP document.
Page 43	ANNEXURE-2: TECHNICAL SPECIFICATIONS	7A) The platform must include a appliance based traffic generator/ simulator which is capable of simulating at least 50,000 attacks with the ability to constantly apply regular updates and additions to the list of attacks.	Kindly remove Traffic genetor "appliance " as this can be done with normal software and the Cyber Range is also a software. However if it is required, please clarify if any integration of the same is required to be done with Cyber range or the traffic generator requirement use case is different to that of Cyber range.	As per RFP.
Page 43	ANNEXURE-2: TECHNICAL SPECIFICATIONS	e) The appliance must be licensed for handling 11 concurrent Users/ Tenants/ PODs from day one and should be scalable to 25 in future.	Kindly clarify what do you mean by Users? Do you mean that at least 11 instances of the solution will be run from Day one and that should be provisioned from the licensing standpoint and in future scalable to 25?	Please refer to updated clause in Final RFP document.
Page 9	SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES	Required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC).	Will RSDC provide the Server to host the software solution ?Does bidder need to provide the specification of the hardware required? If OEM needs Bare metal server will that be provided? Also at one point in RFP it is also asked that bidder has to provide required hardware, please clarify as it is contradictory in RFP.	Please refer to updated clause in Final RFP document.
Page 42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	Of 11 concurrent Users/ Tenants/ PODs, 10 should be based on open-source versions while 1 with OEM specific version (preferably OEM's academic version, if any) for which RISL share separately provide the list of existing OEMs (whose products are installed in RSDC/ RSOC) to the prospective OEMs/ Bidders (on request from the date of NIB and before the last date of bidding).	Kindly clarify what do you mean by Users? Do you mean that at least 11 instances of the solution will be run from Day one and that should be provisioned from the licensing standpoint and in future scalable to 25?	Please refer to updated clause in Final RFP document.
Page 42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	6. b) It must provide isolation from the Internet and must be able to function in an air-gap environment.	Certain upgrades for Subscription based softwares need internet to update patches/ upgrades if any, please consider to relax air-gap environment.	As per RFP.

	44	ANNEXURE-2: TECHNICAL SPECIFICATIONS	It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	Does Bidder need to quote for all the software in the list for the Cyber range?	Please refer to updated clause in Final RFP document.
	42	Point 5, J	It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	We recommend removing below items from the 3rd party list. These products do not have more significance towards the cyber range project. EPP, DAM, Network Forensics, NAC, Cloud Services/ Infra, URL/ Content Filtering, Authentication Authorisation Accounting (AAA).	Please refer to updated clause in Final RFP document.

	43	Point 9, c	It must provide vendor-specific assessments for network security controls including (but not limited to): - Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. etc.	Please remove NAC/AAA. Request more information about DAM assessments and its objective.	Please refer to updated clause in Final RFP document.
		Qyery by email dated 13-03-2023		Will RISL provide all necessary h/w infra required for total tenant counts as well? Currently user/tenant count are asked for 10+1. Please clarify.	Please refer to updated specifications in Final RFP document.
		Qyery by email dated 13-03-2023		Whether bidder has choice of recommending configuration for physical hardware as per Solution requirement as per OEM or RISL will provide the standard configuration hardware for deployment.	Please refer to updated specifications in Final RFP document.
5	38	6.1 Payment Terms and Schedule	76% of the quoted CAPEX after deducting Liquidated Damages, if any. 24% of the remaining CAPEX in 12 quarterly equated installments	Request you to please release the 24% of the remaining CAPEX against the submission of same value of Bank Guarantee valid till project expiry as this will help in to ignoring the interest cost for 12 quarterly equated installments .	Please refer to updated clause in Final RFP document.
	8	5. Certifications	The bidder must possess at the time of bidding, a valid and latest standard/version of: - a. ISO 9001 Certification b. ISO 20000 Certification c. ISO 27001 Certification	The bidder must possess at the time of bidding, a valid and latest standard/version of: any two- a. ISO 9001 Certification b. ISO 20000 Certification c. ISO 27001 Certification	Please refer to updated clause in Final RFP document.
	10	B.1	b) Milestones, Timelines & Deliverables-T+8 Weeks	we request RISL to extend the delviery time line from 8 weeks to 12 weeks and after 12 weeks of delivery please provide 4 weeks more for installtion.	Please refer to updated clause in Final RFP document.
	32	29	29) Warranty a) The bidder must supply all items(hardware as well as software) with comprehensive on-site OEM warranty valid for five years after the goods, or any portion thereof as the case may be, have been delivered to, installed and accepted at the final destination(s) indicated in the bidding document. However, if delay of installation is more than a month's time due to the reasons ascribed to the bidder, the warranty shall start from the date of last successful installation of the items covered under the PO.	we request RISL to provide the confirmation that warranty will be started from date of delivery not from installtion.	Please refer to updated clause in Final RFP document.

	General	Site access and permission	All kind of permission/access at site from feasibility check to link delivery will be arranged by customer. Inbuilding internal cable routing in false celling and under POP wall will be in customer scope of work	Yes.
	General	Power and earthing	RACK Space, Proper power supply and earthing arrangement for the bidder network devices will be arranged and maintained by customer.	Yes.
	General	Network equipment safety	All the network equipments delivered by bidder at customer site for the Services should be kept under safe custody by the customer. In case any device found lost or damaged due to customer attribute than customer has to bear the cost for lost/damaged as well as new device.	As per RFP.
	General	Site readiness	Customer has to ensure the site readiness before bidder depute engineer at site for installation. Delay due to site readiness will not be consider under the delivery time lines and no penalty or LD will be applicable on bidder.	As per RFP.
41		The proposed platform (Cyber Range Platform & associated H/w and S/w components) must be a purpose-built COTS product offering from a reputed OEM dealing in Cyber Security products and services	It should support Virtual/hardware Platform	Please refer to updated clause in Final RFP document.
9	2.II	Modification of existing pre-packaged scenarios and creation of custom (user-defined) scenarios including network and other related H/w and S/w infrastructure as per requirements of RISL/ DoIT&C.	Request RISL to provide more input reqarding custom define scenarios	Please refer to updated clause in Final RFP document.
9	2.III	Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement.	Request RISL to provide details of Existing security OEM /make /Model to check the Integration capablities with offerd solution	Please refer to updated clause in Final RFP document.
9	2.I	Supply, Install, Configure, Customise, Integrate, Test, provide Training and Commission the overall platform at RSDC, Jhalana Dungri, Jaipur, Rajasthan. Required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC).	Request RISL to provide minimum benchmarking for the base line infra of Cyber Range and Training modules/certifcation/Skill details	Please refer to updated clause in Final RFP document.
10	2.vii.	To ensure that the deployment is as per best practices and industry standards, it is mandatory that the Installation, Configuration, Customisation, Integration, Testing, Training and Commissioning of the Platform be done only by respective OEM. Hence, OEM's professional services should be bundled in the proposal.	Request RISL to incoprate SI Implemenation capablities along with OEM PS should fctor for critical components og Cyber Range	As per RFP.
41	3	a) All the essential H/w & S/w components required to use the platform to its full capabilities must be included in the offering. b) It should include all required power and network cables, connectors and accessories	request RISL to mention minimum benchmarking of the platform	As per RFP.

42	Point 5, J	It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	We recommend removing below items from the 3rd party list. These products do not have more significance towards the cyber range project. EPP, DAM, Network Forensics, NAC, Cloud Services/ Infra, URL/ Content Filtering, Authentication Authorisation Accounting (AAA).	Please refer to updated clause in Final RFP document.
43	Point 9, c	It must provide vendor-specific assessments for network security controls including (but not limited to): - Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. etc.	Please remove NAC/AAA. Request more information about DAM assessments and its objective.	Please refer to updated clause in Final RFP document.
9	Phase-1: Commissioning the Cyber Range Platform (hereinafter referred as Platform) Point No 2 (i)	Supply, Install, Configure, Customise, Integrate, Test, provide Training and Commission the overall platform at RSDC, Jhalana Dungri, Jaipur, Rajasthan. Required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC).	Kindly confirm if RISL will take full responsibility of the associated hardware and software infrastructure components.It is recommend OEM to take responsibility their respective products and required VM infra or appliances should be quoted along so that there is no issue in support or compatibility.	Please refer to updated clause in Final RFP document.
9	Phase-1: Commissioning the Cyber Range Platform (hereinafter referred as Platform) Point No 2 (ii)	Modification of existing pre-packaged scenarios and creation of custom (user-defined) scenarios including network and other related H/w and S/w infrastructure as per requirements of RISL/ DoIT&C.	Pre packed scenarios may/may not be useful to RISL/DoIT&C and scope of custom scenario is not mentioned in the RFP. Creating custom scenario need OEM Expertise & OEM man hour for configuration etc hence directly related to cost. Kindly specificy scenarios required for competitive bidding.	Please refer to updated clause in Final RFP document.

9	Phase-1: Commissioning the Cyber Range Platform (hereinafter referred as Platform) Point 2(iii)	Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement	11th POD is already a production replica hence request to delete this clause, else this will defeat the purpose of the Cyber Range R&D platform/Lab.	Please refer to updated clause in Final RFP document.
10	Phase-2: Operate and Maintain (O&M) Cyber Range Platform (Three Years) Point No 3.	Operations & Maintenance of the deployed platform would be required for an initial period of Three years from the date of commissioning (Go-Live) and if required, could be extended for another period of Two years on mutual acceptance and as per rates mentioned in RISL's work order issued earlier to the successful bidder.	Price variation is expected from the date of bidding till 5 years and we also need to consider dollar inflation hence the extension may be done keeping this in consideration at the Future Market value and not current market value .	Please refer to updated clause in Final RFP document.
	Phase-2: Operate and Maintain (O&M) Cyber Range Platform (Three Years) Point No (vii)	Regular review of integrations and fix them for issues reported, if any, in co-ordination with respective stakeholders.	It is recommended that OEM engagement should be made mandatory for fixed no of period, as this will be cost optimised way of fulfilling the requirement. Hence this may be changed to "regular review of integration and fix of issues reported will be done twice a year by OEM experts"	As per RFP.
10	Phase-2: Operate and Maintain (O&M) Cyber Range Platform (Three Years) Point No (x)	Conduct periodic security control assessments of existing production infra in RSDC + RSOC and provide the assessment reports with deviations and recommended controls, policies and configurations to be updated/implemented.	We understand this will be done by the manpower (one /year) deployed for this project at RISL, as this is the optimised way of fulfilling the requirement.	As per RFP.
10	Milestones, Timelines & Deliverables Point No (b)	Successful completion of Phase-1 as per Section 4-a-2 above ,T+8 Weeks	Delivery of hardware may take time, hence request extension to T+16 weeks.	Please refer to updated clause in Final RFP document.
41	Annexure 2 Technical Specifications Point No 4 (a)	It must support at least 11 Concurrent Users/ Tenants/ PODs from day one and should be scalable to 25 in future.	Open source solutions have challenge in terms of integration,configuration and suppport.Also creating scenarios from open source solution is challenging.We also understand that RISL want to offer training on every platform possible hence request to break the PODS as below: 1. 5 OEM specific PODS, if possible kindly mention some technical requiremenrt of individual products for competitive bidding. 2. 5 Open Source products. 3. 1 RSOC production POD. Also we need to define scenario only for OEM specifics PODS and for remaning PODS declration has to be submited by the bidder on what all scenario are they offering.	Please refer to updated clause in Final RFP document.
42	Annexure 2 Technical Specifications Point No 6 (b)	It must provide isolation from the Internet and must be able to function in an air-gap environment.	Solution offering from all the OEM's has changed and it is not possible for solution to operate in air gap environemt as management and upgrades are done from the cloud. Kindly delete this clause.	As per RFP.
43	Annexure 2 Technical Specifications Point No 7 (a)	The platform must include a appliance based traffic generator/ simulator which is capable of simulating at least 50,000 attacks with the ability to constantly apply regular updates and additions to the list of attacks.	As traffic generator/simulator is common for all the PODS hence kindly provide technical specifications for the same for competitive bidding. There are not many OEM for traffic generator hence OEM can favour some bidders.Hence request if cost discover of this component can be done and communicated to all the bidders.	As per RFP.

	42	Annexure 2 Technical Specifications Point No 5 (k)	For creating a heterogeneous environment, at least two different products (one open- source + one OEM specific) for each of the above category should be included in offering	Kindly remove this clause.	Please refer to updated clause in Final RFP document.
		Additonal Clause		The winning bid should include QCBS marking also as this is not a product based RFP. All the solutions/stack to be duly validated before declaring winning bidder.	As per RFP.
6	8	Technical Capability	The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC) OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 6 Crores each.	The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC)/Provided security solution OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform Or within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 5 Crores each.	Please refer to updated clause in Final RFP document.
	8	Technical Manpower	The Bidder should have at least 10 full-time permanent employees on his payroll with any of the following valid certifications: - 1. Certified Information System Security Professional (CISSP) 2. Certified Information System Auditor (CISA) 3. Certified Information Systems Manager (CISM) 4. Offensive Security Certified Professional (OSCP) 5. Certified Ethical Hacker (CEH) 6. any other Cyber Security related certification from a reputed global organisation	The Bidder should have at least 10 full-time permanent employees on his payroll or provide the undertaking that the bidder will provide employees' details within 60 days after the bid is awarded. with any of the following valid certifications: - 1. Certified Information System Security Professional (CISSP) 2. Certified Information System Auditor (CISA) 3. Certified Information Systems Manager (CISM) 4. Offensive Security Certified Professional (OSCP) 5. Certified Ethical Hacker (CEH) 6. any other Cyber Security related certification from a reputed global organisation	As per RFP.
	8	Financial Net Worth	The net worth of the bidder, as on 31st March 2021, should be Positive	Since the project value is 30 cr, we are suggesting that you, please ask the positive net worth should be a minimum of 15 cr the bidder, this will help to smooth execution for the bidder and that will also show the financial credential is good for the bidder.	As per RFP.
	38	Payment Terms and Schedule	76% of the quoted CAPEX after deducting Liquidated Damages, if any.	Requesting you release the 85% payment of capex value after the Successful commissioning of the overall Cyber Range Platform and the Remaining 15% of Order Value, in equated installments payable at the end of each year, however, if the bidder submitted the BG the same amount then the same amount will be also released after 3 months of go live.	Please refer to updated clause in Final RFP document.

	42	Point 5, J	It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	We recommend removing below items from the 3rd party list. These products do not have more significance towards the cyber range project. EPP, DAM, Network Forensics, NAC, Cloud Services/ Infra, URL/ Content Filtering, Authentication Authorisation Accounting (AAA).	Please refer to updated clause in Final RFP document.
	43	Point 9, c	It must provide vendor-specific assessments for network security controls including (but not limited to): - Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. etc.	Please remove NAC/AAA. Request more information about DAM assessments and its objective.	Please refer to updated clause in Final RFP document.

	43	Point 9, c	It must provide vendor-specific assessments for network security controls including (but not limited to): - Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. etc.	Please remove NAC/AAA. Request more information about DAM assessments and its objective.	Please refer to updated clause in Final RFP document.
	38	Platform Uptime Service Levels	100% of quarterly payable OPEX. Note: - Two such consecutive quarterly events shall be treated as breach of contract	Request you to please change the penalty clause should be higher side maximum of 10 % of the contract value.	Please refer to updated clause in Final RFP document.
	10	Milestones, Timelines & Deliverables	T+8 Weeks : □ OEM(s) License & Support Certificates/ Letters/ Undertakings	Requesting to minimum T+12 Weeks minimum require	Please refer to updated clause in Final RFP document.
7	41	b	At the time of bidding, OEM must have: - i. A valid ISO 9001, ISO 20000 and ISO 27001 certification ii. Its own operational SOC anywhere across the globe iii. A direct support centre in India iv. Full-time Cyber Security Researchers (at least 50) v. Established Incident Response (IR) Service vi. At least one successful deployment (proposed platform) in India in last Five years (from the start date of bidding).	We request if these conditions would also be extended to Bidders and not just limited to OEM as Cyberbit being CyberRange OEM would like to bid along with their partenrs who can adhere to all below listed eligibility criterieas. i.e Revised clause - At the time of bidding, OEM / Bidder must have: - i. A valid ISO 9001 and ISO 27001 certification ii. Its own operational SOC anywhere across the globe iii. A direct support centre in India iv. Full-time Cyber Security Researchers (at least 50) v. vi. At least five successful deployment (proposed platform) in India in last Five years (from the start date of bidding).	Please refer to updated clause in Final RFP document.
	41	a	It must be an on-premise solution with perpetual licenses of all required Hardware and Software components supplied with a Three (3) Year OEM Warranty and Premium Support (24x7x365).	Offering premium support is too costly for a training platform. We suggest that if OEM Warranty and Premium Support can be changed to Office Hours instead of 24x7x365 for a total duration of 3 years contract.	Please refer to updated clause in Final RFP document.
	41	a	It must support at least 11 Concurrent Users/ Tenants/ PODs from day one and should be scalable to 25 in future.	Instead of present clause , we would like to suggest a change which will make this setup more commerciably viable and better ROI. Suggestion - Change the concurrency of training to be 2 with up to 20 users in each session and commit for future expension if there will be additional future demand.	Please refer to updated clause in Final RFP document.

	41	a	It must include all the essential pre-packaged scenarios (at least 50, categorized by type and complexities and searchable too) along with varying difficulty levels and step-by-step documentation/ guide with visual representation of corresponding layer for each scenario so as to facilitate a variety of real-world simple-medium-complex exercises in an isolated and sandboxed environment. Also, looking to rapidly	It must include all the essential pre-packaged scenarios (at least 50, categorized by type and complexities and searchable too, mapped according to MITRE ATTACK framework) along with varying difficulty levels and step-by-step documentation/ guide with visual representation of corresponding layer for each scenario so as to facilitate a variety of real-world simple-medium-complex exercises in an isolated and sandboxed environment. Also, looking to rapidly changing Cyber Security Threat landscape, it is must that new pre-packaged	Please refer to updated clause in Final RFP document.
	42	j	It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	It must include both logical OR physical network components (virtualised/physical), wherever applicable and relevant to the attack scenario, including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	Please refer to updated clause in Final RFP document.
	42	k	For creating a heterogeneous environment, at least two different products (one open-source + one OEM specific) for each of the above category should be included in offering.	For cost effectiveness reasons, we suggest to remove this clause.	Please refer to updated clause in Final RFP document.
	42	l	Of 11 concurrent Users/ Tenants/ PODs, 10 should be based on open-source versions while 1 with OEM specific version (preferably OEM's academic version, if any) for which RISL share separately provide the list of existing OEMs (whose products are installed in RSDC/ RSOC) to the prospective OEMs/ Bidders (on request from the date of NIB and before the last date of bidding).	Instead of present clause , we would like to suggest a change which will make this setup more commerciably viable and better ROI. Suggestion - Change the concurrency of training to be 2 with up to 20 users in each session and commit for future expension if there will be additional future demand. Please provide the list of RISL existing tools for referance. The network shall allow integration of RISL tools as possible.	Please refer to updated clause in Final RFP document.
	42	o	Platform must also provide REST APIs for automation and integration with third-party systems and applications.	Platform must all for integration with third-party systems and applications.	Please refer to updated clause in Final RFP document.
	43	a	The platform must include a appliance based traffic generator/ simulator which is capable of simulating at least 50,000 attacks with the ability to constantly apply regular updates and additions to the list of attacks.	The platform must include a traffic generator/ simulator which is capable of simulating large number of traffics or malicious traffic with the ability to constantly apply regular updates and additions to the list of attacks.	As per RFP.
	43	e	The appliance must be licensed for handling 11 concurrent Users/ Tenants/ PODs from day one and should be scalable to 25 in future.	The appliance must be licensed to support the initial setup and should be scalable in future.	Please refer to updated clause in Final RFP document.

8	9	a) Scope of Work (SoW) Details	Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement.	As per respective RFP clauses it has been asked to build a cyber range platform as per NIST's NICE framework by incorporating/replicating existing security layers running in existing datacenter /SOC environment including NIPS, HIPS, Anti APT, endpoint security to achieve traffic generation and threat emulation scenarios. Please help for providing complete details on eixtsing security products with their make & model so that bidders can incorporate existing security components running in SDC/SOC environment of respective OEMs to build cyber range platform as a part of solution offering.	Please refer to updated clause in Final RFP document.
	10	3) Phase-2: Operate and Maintain (O&M) Cyber Range Platform (Three Years)	v. To ensure the timely updation/upgradation of the overall platform and associated components as and when released by respective OEM(s) with prior approval from RISL/ DoIT&C. vi. Integrations with existing and new appliances deployed in RSDC & RSOC throughout the project duration as per purchaser's and/ or platform requirement.		
	41	ANNEXURE-2: TECHNICAL SPECIFICATIONS	a) The proposed platform (Cyber Range Platform & associated H/w and S/w components) must be a purpose-built COTS product offering from a reputed OEM dealing in Cyber Security products and services. a) All the essential H/w & S/w components required to use the platform to its full capabilities must be included in the offering.		
	42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	j) It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc. k) For creating a heterogeneous environment, at least two different products (one open-source + one OEM specific) for each of the above category should be included in offering.		

9	8	2. PRE-QUALIFICATION/ ELIGIBILITY CRITERIA FOR BIDDER Sr. No. 4 Technical Capability	The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC) OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, the bidder may submit details of two projects of Rs. 6 Crores each.	Request you to kinldy consider: The bidder must have successfully commissioned at least one/two project(s) of: - Establishing Security Operation Center (SOC) OR Providing services as Managed Security Service Provider (MSSP) OR Cyber Security Training using Cyber Range Platform within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 8 Crores. Alternatively, the bidder may submit details of two projects of Rs. 6 Crores each.	Please refer to updated clause in Final RFP document.
	8	2. PRE-QUALIFICATION/ ELIGIBILITY CRITERIA FOR BIDDER Sr. No. 5 Certifications	The bidder must possess at the time of bidding, a valid and latest standard/version of: - a. ISO 9001 Certification b. ISO 20000 Certification c. ISO 27001 Certification	Request you to please consider: The bidder must possess atleast 2 out of the below 3 certifications at the time of bidding, a valid and latest standard/version of: - a. ISO 9001 Certification b. ISO 20000 Certification c. ISO 27001 Certification	Please refer to updated clause in Final RFP document.
	9	3. SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES Sr. No a) 2) i)	Required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC).	You are requested to kindly confirm whether the required hardware shall be provided by RISL or needs to be procured by the bidder. If it is under bidder's scope, please confirm and also include a line item in the cost sheet.	Please refer to updated clause in Final RFP document.
	38	SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT Sr. No. 1	76% of the quoted CAPEX after deducting Liquidated Damages, & 24% of the remaining CAPEX in 12 quarterly equated installments	Request you to kindly give the 100% capex before the start of the Opex period and amend the payment terms as below: 100 % of the Hardware cost will be paid after delivery of hardware. 100 % of the Software cost will be paid after delivery of licence.	Please refer to updated clause in Final RFP document.
10	9	3-a-2-i	Supply, Install, Configure, Customise, Integrate, Test, provide Training and Commission the overall platform at RSDC, Jhalana Dungri, Jaipur, Rajasthan. Required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC).	Please clarfiy if Server Hardware will be provided by RISL/DoIT&C(RSDC)	Please refer to updated clause in Final RFP document.
	10	3-b-1	Successful completion of Phase-1 as per Section 4-a-2 above.	Request to change the timeline to 20 Weeks as hardware delivery take approx 8-10 weeks	Please refer to updated clause in Final RFP document.
	9	3-a-2-iii	Integration of the platform with target production infrastructure i.e., existing Rajasthan State Data Centre (RSDC) appliances and RSOC security appliances which includes Routers, Switches, Firewall, IPS/IDS, DDoS, ADC, Web Security, Email Security, WAF, APT, SIEM NBAD, SOAR etc. as per purchaser's requirement.	Request to provide the list of Security infra with make & Model so that simulation environment can be created using same set of vitual appliances.	Please refer to updated clause in Final RFP document.
	64	Annexure 16	Platform Engineer: Masters (M.Sc./ MCA/ MTech.) Degree in Computer Science/ Information Technology/ Cyber Security	Request to consider B.Tech/B.E also as MCA is considered as equivalent to B.Tech / B.E	Please refer to updated clause in Final RFP document.

41	b	At the time of bidding, OEM must have: - i. A valid ISO 9001, ISO 20000 and ISO 27001 certification ii. Its own operational SOC anywhere across the globe iii. A direct support centre in India iv. Full-time Cyber Security Researchers (at least 50) v. Established Incident Response (IR) Service vi. At least one successful deployment (proposed platform) in India in last Five years (from the start date of bidding).	We request if these conditions would also be extended to Bidders and not just limited to OEM as Cyberbit being CyberRange OEM would like to bid along with their partenrs who can adhere to all below listed eligibility criterieas. i.e Revised clause - At the time of bidding, OEM / Bidder must have: - i. A valid ISO 9001 and ISO 27001 certification ii. Its own operational SOC anywhere across the globe iii. A direct support centre in India iv. Full-time Cyber Security Researchers (at least 50) v. vi. At least five successful deployment (proposed platform) in India in last Five years (from the start date of bidding).	Please refer to updated clause in Final RFP document.
41	a	It must be an on-premise solution with perpetual licenses of all required Hardware and Software components supplied with a Three (3) Year OEM Warranty and Premium Support (24x7x365).	Offering premium support is too costly for a training platform. We suggest that if OEM Warranty and Premium Support can be changed to Office Hours instead of 24x7x365 for a total duration of 3 years contract.	Please refer to updated clause in Final RFP document.
41	a	It must support at least 11 Concurrent Users/ Tenants/ PODs from day one and should be scalable to 25 in future.	Instead of present clause , we would like to suggest a change which will make this setup more commerciably viable and better ROI. Suggestion - Change the concurrency of training to be 2 with up to 20 users in each session and commit for future expension if there will be additional future demand.	Please refer to updated clause in Final RFP document.
41	a	It must include all the essential pre-packaged scenarios (at least 50, categorized by type and complexities and searchable too) along with varying difficulty levels and step-by-step documentation/ guide with visual representation of corresponding layer for each scenario so as to facilitate a variety of real-world simple-medium-complex exercises in an isolated and sandboxed environment. Also, looking to rapidly changing Cyber Security Threat landscape, it is must that new pre-packaged scenarios, as per prevailing threat landscape, be updated by respective OEMs throughout the project duration.	It must include all the essential pre-packaged scenarios (at least 30, categorized by type and complexities and searchable too, mapped according to MITRE ATTACK framework) along with varying difficulty levels and step-by-step documentation/ guide with visual representation of corresponding layer for each scenario so as to facilitate a variety of real-world simple-medium-complex exercises in an isolated and sandboxed environment. Also, looking to rapidly changing Cyber Security Threat landscape, it is must that new pre-packaged scenarios, as per prevailing threat landscape, be updated by respective OEMs throughout the project duration.	Please refer to updated clause in Final RFP document.

42	j	It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	It must include both logical OR physical network components (virtualised/physical), wherever applicable and relevant to the attack scenario, including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	Please refer to updated clause in Final RFP document.
42	k	For creating a heterogeneous environment, at least two different products (one open-source + one OEM specific) for each of the above category should be included in offering.	For cost effectiveness reasons, we suggest to remove this clause.	Please refer to updated clause in Final RFP document.
42	l	Of 11 concurrent Users/ Tenants/ PODs, 10 should be based on open-source versions while 1 with OEM specific version (preferably OEM's academic version, if any) for which RISL share separately provide the list of existing OEMs (whose products are installed in RSDC/ RSOC) to the prospective OEMs/ Bidders (on request from the date of NIB and before the last date of bidding).	Instead of present clause , we would like to suggest a change which will make this setup more commerciably viable and better ROI. Suggestion - Change the concurrency of training to be 2 with up to 20 users in each session and commit for future expension if there will be additional future demand. Please provide the list of RISL existing tools for referance. The network shall allow integration of RISL tools as possible.	Please refer to updated clause in Final RFP document.
42	o	Platform must also provide REST APIs for automation and integration with third-party systems and applications.	Platform must all for integration with third-party systems and applications.	Please refer to updated clause in Final RFP document.
43	a	The platform must include a appliance based traffic generator/ simulator which is capable of simulating at least 50,000 attacks with the ability to constantly apply regular updates and additions to the list of attacks.	The platform must include a traffic generator/ simulator which is capable of simulating large number of traffics or malicious traffic with the ability to constantly apply regular updates and additions to the list of attacks.	As per RFP.
43	e	The appliance must be licensed for handling 11 concurrent Users/ Tenants/ PODs from day one and should be scalable to 25 in future.	The appliance must be licensed to support the initial setup and should be scalable in future.	Please refer to updated clause in Final RFP document.
4	Bid Evaluation Criteria	Low Cost Based Selection (LCBS) - Lowest evaluated technically responsive bid.	Request to Change the Criteria for QCBS so that suitable bidder can be shortlisted taking care new inititive by Govt. of Rajasthan in the domain of Cyberrange.	As per RFP.
8	Technical Capability	within Three years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 10 Crores. Alternatively, bidder may submit details of two projects of Rs. 6 Crores each.	within Five years from the bid submission deadline wherein the cost of one project should be equal to or higher than Rs. 20 Crores. Alternatively, bidder may submit details of two projects of Rs. 11 Crores each.	Please refer to updated clause in Final RFP document.

	8	Financial Turnover	Average Annual Turnover of the bidder from IT/ITeS during the Financial years 2018-19, 2019-20, 2020-21 (as per the audited balance sheets), should be at least Rs. 50 Crores.	Average Annual Turnover of the bidder from Information Security/Security Services during the Financial years 2018-19, 2019-20, 2020-21 (as per the audited balance sheets), should be at least Rs. 100 Crores.	As per RFP.
	38	Payment Terms and Schedule	76% of the quoted CAPEX after deducting Liquidated Damages, if any.	85% of the quoted CAPEX after deducting Liquidated Damages, if any. Remaining 15% Can be euated in 3 Years.	Please refer to updated clause in Final RFP document.
11	Page 41	ANNEXURE-2: TECHNICAL SPECIFICATIONS	b) At the time of bidding, OEM must have: - i. A valid ISO 9001, ISO 20000 and ISO 27001 certification	We kindly suggest that OEM should have one of the provided ISO certifcations only	Please refer to updated clause in Final RFP document.
	Page 43	ANNEXURE-2: TECHNICAL SPECIFICATIONS	7A) The platform must include a appliance based traffic generator/ simulator which is capable of simulating at least 50,000 attacks with the ability to constantly apply regular updates and additions to the list of attacks.	Kindly remove Traffic genetor "appliance " as this can be done with normal software and the Cyber Range is also a software. There is always a BAS included which has attack signatures, and hence traffic generator need not have 50,000 attacks. Kindly remove as this is restrictive and points to One OEM	As per RFP.
	Page 43	ANNEXURE-2: TECHNICAL SPECIFICATIONS	e) The appliance must be licensed for handling 11 concurrent Users/ Tenants/ PODs from day one and should be scalable to 25 in future.	Kindly clarify what do you mean by Users? Do you mean that at least 11 instances of the solution will be run from Day one and that should be provisioned from the licensing standpoint and in future scalable to 25?	Please refer to updated clause in Final RFP document.
	Page 9	SCOPE OF WORK, MILESTONES, TIMELINES & DELIVERABLES	Required Server Hardware (Physical Server/ Virtual Machines) would be provided by RISL/ DoIT&C (RSDC).	Will RSDC provide the Server to host the software solution ?Does bidder need to provide the specification of the hardware required? If OEM needs Bare metal server will that be provided?	Please refer to updated clause in Final RFP document.
	Page 42	ANNEXURE-2: TECHNICAL SPECIFICATIONS	Of 11 concurrent Users/ Tenants/ PODs, 10 should be based on open-source versions while 1 with OEM specific version (preferably OEM's academic version, if any) for which RISL share separately provide the list of existing OEMs (whose products are installed in RSDC/ RSOC) to the prospective OEMs/ Bidders (on request from the date of NIB and before the last date of bidding).	Kindly clarify what do you mean by Users? Do you mean that at least 11 instances of the solution will be run from Day one and that should be provisioned from the licensing standpoint and in future scalable to 25?	Please refer to updated clause in Final RFP document.
	44	ANNEXURE-2: TECHNICAL SPECIFICATIONS	It must include both logical and physical network components (virtualised/physical), wherever applicable including (but not limited to) Switches, Routers, Next-generation Firewall (NGFW), Web Application Firewall (WAF), Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Distributed Denial of Service (DDoS), Data Loss Prevention (DLP) system, URL/ Content Filtering, Endpoint Detection and Response (EDR), Endpoint Protection Platform (EPP), Antivirus, and Malware Sandboxing, Email Security, DNS Security, Cloud Services/ Infra, Security Information and Event Management (SIEM), Advanced Persistent Threat (APT), Network Analytics, Network Access Control (NAC), Authentication Authorisation Accounting (AAA), Database Activity Monitoring (DAM), Network Forensics, Web Proxy etc. + nodes and infrastructure including (but not limited to) Web Servers, App Servers, Database Servers, File Servers, Workstations etc.	Request for clarification.. Does Bidder need to quote for all the software in the list for the Cyber range?	Please refer to updated clause in Final RFP document.