Ref: CO-ERM/IT/CSD/Modification-1 **Date: 14.07.2025**

Modification – 1: On-boarding Cyber Security Knowledge Partners for Awareness Training sessions for Employees, Agents, Vendors, Customers and other Stakeholders

Reference No.: CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June, 2025

This is with reference to the RFP released by the Life Insurance Corporation of India on 18th June, 2025 captioned above. Further modifications to this RFP are given below:

SL NO	BID DOCUMENT PAGE NO., CLAUSE NO.	ORIGINAL TENDER CONDITION	MODIFICATIONS/REVISED CONDITION (INDICATED IN BOLD)
1.	Page-13 6. Eligibility Criteria Sl. No.7	Bidder should have at least 5 personnel on their payroll who have relevant experience in imparting various awareness sessions/trainings as given in the RFP. Any Graduate with at least two certification out of CISA, OSCP, CISSP.C/PENT, CISM, CEH.	Bidder should have at least 5 personnel on their payroll who have relevant experience in imparting various awareness sessions/trainings as given in the RFP. Any Graduate with at least one certification out of CISA, OSCP, CISSP, C/PENT, CISM, CEH.
2.	Page-13 4.Technical Bid Sl. No.4 (iv) **AND** Page-45 Section E: Scope of Services Sl no. III. Software to be provided for learning management system (LMS)	The bidder must supply a thorough inventory of the hardware components required for the planned implementation. This bill of Quantity (BOQ) as per Annexure J should be itemized separately for all the environments, including DC, UAT and Disaster Recovery (DR). The BOQ should include, but is not limited to, the following details: ✓ In Scope solutions Components ✓ Site/Environment ✓ OS name other than RHEL with no. of licenses to be provided ✓ DB name and its version with no. of licenses to be provided ✓ CPU/Core required ✓ VLAN requirement (VLAN or Internet) ✓ RAM ✓ Hard Disk Size ✓ Any other Software pre-requisites (.NET framework, IIS, IE, any other OS services, etc.) are required to be provided.	LIC will provide licenses for Red Hat Enterprise Linux (RHEL) and the MySQL database. Physical servers are not allowed. Load balancing feature of private cloud will be provided by LIC. LIC will provide virtual servers from its private cloud infrastructure as per the specifications provided by the successful bidder and approved by LIC. The bidder must supply a thorough inventory of the hardware components required for the planned implementation. This bill of Quantity (BOQ) as per Annexure J should be itemized separately for all the environments, including DC (production), UAT and Disaster Recovery (DR). The BOQ should include, but is not limited to, the following details: ✓ In Scope solutions Components ✓ Site/Environment ✓ OS name other than RHEL with no. of licenses to be provided ✓ DB name other than MySQL and its version with no. of licenses to be provided ✓ CPU/Core required ✓ VLAN requirement (VLAN or Internet) ✓ RAM ✓ Hard Disk Size ✓ Any other Software pre-requisites (.NET framework, IIS, IE, any other OS services, etc.) are required to be provided by the successful vendor.

SL NO	BID DOCUMENT PAGE NO., CLAUSE NO.	ORIGINAL TENDER CONDITION	MODIFICATIONS/REVISED CONDITION (INDICATED IN BOLD)
			The responsibility for hardware sizing for the proposed solution shall lie entirely with the successful bidder, taking into account the requirements for Development/Testing (UAT), Production (DC), and Disaster Recovery (DR) environments. The bidder must provide detailed justification and supporting documentation for the proposed sizing. The infrastructure and application should be sized to take care the following: (a) at least 15 lakh agents with 5 % growth (b) 1 (one) lakh employees and (c) 10000 vendors Other details are given below: Concurrent Users : at least 20000 per second Maximum users: at least 50000 CPU utilization: not more than 60 % with a threshold of 80 % 3-tier architecture (Web/App/DB) with high availability will be responsibility of successful bidder by following secure software development life cycle. If the selected vendor proposes the use of any alternative software licenses other than RHEL and MySQL, such licenses shall be provided by the vendor, in alignment with the scope of this RFP. Furthermore, any additional software licenses required for the successful implementation, deployment, and day-to-day operations/management of platform etc. of the proposed LMS platform shall be the sole responsibility of the selected vendor. All software components proposed and used for this project shall adhere to the latest stable versioning practices, following (N-1) version policy, where N is the latest version of the software at the time of implementation ensuring compatibility, vendor support, and alignment with industry best practices.
3.	Page-56 **Section G: Payment Terms and Conditions**	Milestone basis payment terms and conditions included.	Revised payment terms and conditions in pdf format
4.	Page-69 **Annexure C: Eligibility**	The Bidder during the last 5 years(starting from 01.04.2020) from the date of this RFP should be a knowledge partner for providing	Deleted due to repetition.

SL NO	BID DOCUMENT PAGE NO., CLAUSE NO.	ORIGINAL TENDER CONDITION	MODIFICATIONS/REVISED CONDITION (INDICATED IN BOLD)
	Criteria Sl no. 6	awareness sessions/trainings related to cyber security at minimum 5 organisations in PSU /Government /Private /BFSI Sector / University in India. **Refer to Appendix 2**	
5.	Page-68 – Annexure C	Annexure-C	Revised-Annexure C in pdf format enclosed.
6.	Page-72- Annexure D	Annexure-D	Revised-Annexure D in pdf format enclosed.
7.	Annexure-C	Eligibility Bid-Knowledge Partners-V1.0.xls	Eligibility Bid-Knowledge Partners-V1.1.xls
8.	Annexure-D	Technical Bid-Knowledge Partners-V1.0.xls	Technical Bid-Knowledge Partners-V1.1.xls
9.	Annexure-F	Commercial Bid Document-Knowledge Partner-V1.0.xls	Commercial Bid Document-Knowledge Partner-V1.1.xls
10.	Page -11	Last date of Submission of bids 18th July 20525, latest by 4 PM	Last date of Submission of bids 30th July 2025, latest by 4 PM
11.	Page -11	Bid Opening date and time 18th July 20525, latest by 4.15 PM	Bid Opening date and time 30th July 20525, latest by 4.15 PM

These amendments will form a part of the RFP for On-boarding Cyber Security Knowledge Partners for Awareness Training sessions for Employees, Agents, Vendors, Customers and other Stakeholders of Reference No.: CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June 2025. All the bidders are requested to take note of the amendments and respond accordingly.

Bidders have to use the revised & new formats for filling up the required information. Please note that, if the same has not been done, the bid is liable to be rejected.

Enclosures:

1. Modification – 1
2. Response to bidders' pre-bid queries
3. Revised Eligibility Bid workbook (Eligibility Bid-Knowledge Partners-V1.1.xls)
4. Revised Technical Bid Workbook (Technical Bid-Knowledge Partners-V1.1.xls)
5. Revised Commercial bid workbook (Commercial Bid Document-Knowledge Partner-V1.1.xls)
6. Addendum-1: Revised Annexure-C and Revised Annexure-D
7. Addendum-2: Mile stone based payments included in Section G
8. Pre-bid meeting presentation

Executive Director (ERM) & CRO

भारतीय जीवन बीमा निगम
LIFE INSURANCE CORPORATION OF INDIA

Addendum-1: Revised Annexure-C and Revised Annexure-D

Revised: Annexure-C and Annexure-D

This is with reference to the RFP released by the Life Insurance Corporation of India on 18th June, 2025 captioned above. Further modifications to this RFP are given below:

Annexure C: Eligibility Criteria (Revised)

SN	Eligibility Criteria	Documents to be Submitted
1.	The Bidder should be a registered legal entity in India. **Refer to Appendix 1**	Copy of the Certificate of Incorporation issued by Registrar of Companies and full address of the registered office.
2.	The Bidder should hold a valid GST registration and PAN Card. **Refer to Appendix 1**	Attested copies of documentary proof.
3.	The Bidder should have a minimum annual turnover of Rs 20 Crores in previous three financial years (2022-2023, 2023-2024 and 2024-2025). For bidder applying under MSME the bidder should have a minimum annual turnover of Rs 1 Crore in previous three financial years (2022-2023, 2023-2024 and 2024-2025). **Refer to Appendix 1**	Audited Financial statements / balance sheet /CA Certificate for the respective financial years. Bidders should submit relevant MSME/NSIC certificate in the envelope as mentioned in this RFP document.
4.	The Bidder should have a positive net worth in previous three financial years (2022-2023, 2023-2024 and 2024-2025). **Refer to Appendix 1**	Audited Financial statements / balance sheet /CA Certificate for the respective financial years.
5.	The bidder should have handled assignments/ Services related to cyber security trainings/ Awareness Training sessions and content development to Regulator/BFSI/PSU/any university in India /any other large organization in India during last three financial years [i.e. (2022-2023, 2023-2024 and 2024-2025]. The bidder should have experience in handling training in at least 3 of the following areas: Case Studies on Recent Cyber Security Breaches; Cyber Security Framework; Information Security Policies; Cyber Security related regulatory guidelines; Information Security Awareness Training; Cyber Hygiene; Cyber Security Governance; Cyber security diploma / degree program affiliated with any university in India; Cyber Security related regulatory guidelines; Data Protection and Privacy; Digital Personal Data Protection Act, 2023; Certified ethical hacking course covering (Endpoint Security, Email Security, Physical Security etc.) Secure coding practices Certified training programs like CISSP/CISA/CISM/CEH	Audited Financial statements / balance sheet /CA Certificate for the respective financial years.

SN	Eligibility Criteria	Documents to be Submitted
	IT/ Cyber Risk Management; Network Security; Third- Party Risk Management; Vulnerability Management; **Refer to Appendix 2**	
6.	The Bidder during the last 5 years from the date of this RFP should be a knowledge partner for providing awareness sessions/trainings related to cyber security at minimum 5 organisations in PSU /Government /Private /BFSI Sector / University in India. **Refer to Appendix 2**	The bidder should submit details as per format under Annexure C and Annexure E along copies of the Letter of acceptance (LoA) / work order/ contract/ completion certificate/ confirmation email for relevant experience. The project completion date should be within the last 5 years as on the date of this RFP.
7.	Bidder should have at least 5 personnel on their payroll who have relevant experience in imparting various awareness sessions/trainings as given in the RFP. **Any Graduate with at least one certification out of CISA, OSCP, CISSP, C/PENT, CISM, CEH** **Refer to Appendix 3**	CVs of the concerned personnel with details of experience and qualification on company letter head duly signed by the authorized signatory of the bidder. Details to be provided: Name Designation Years of experience Detailed description of experience Qualifications Certificates (if any) Declaration on company letter head duly signed by the authorized signatory of the bidder.
8.	The bidder should have LMS – learning management software either developed by them or partnership with respectable OEM to deliver the requirements of this RFP starting from 01.04.2020. **Refer to Appendix 4**	Declaration on company letter head duly signed by the authorized signatory of the bidder. If partnered with OEM then relationship agreement, duly signed by both the parties and establishing relationship for the minimum of the tenure of this RFP.
9.	The Bidder should not have been blacklisted by Government of India / RBI / SEBI / IRDAI. However, such blacklisting will be null and void for the purpose of bidding in this RFP, if the bidder has obtained stay order in any court of India. **Refer to Annexure-G**	Declaration on company letter head duly signed by the authorized signatory of the bidder.

Note:

- Bidder must comply with the above-mentioned criteria. Non-compliance to any of the criteria may entail rejection of the bid. LIC reserves the right to verify/evaluate the claims made by the bidder independently. Any misrepresentation will entail rejection of the offer.
- Evidence to be submitted for each eligibility criteria should be part of the same response document. Proper naming and indexing should be done to avoid any ambiguity.
- The bidder who successfully qualifies in the eligibility criteria, only their technical bids will be subsequently opened for further evaluation.

Appendices

1. **Appendix 1:**
   a. Copy of the Certificate of Incorporation issued by Registrar of Companies and full address of the registered office.
   b. Attested copies of documentary proof of valid GST registration and PAN Card.
   c. Bidders should submit relevant MSME/NSIC certificate in the envelope as mentioned in this RFP document.

#	Date of issue	Issuing Authority	Address of the Organization	Evidence	Pg. No. in current document
Certificate of Incorporation issued by Registrar of Companies				**E1.1**	
#	**Number**	**Date of issue**			
PAN Card				**E1.2**	
GST registration				**E1.3**	
MSME Certificate				**E1.4**	

- E1: Kindly hyperlink the respective Evidence in above table
- E2: Kindly hyperlink the respective Evidence in above table
- …

a. The Bidder should have a minimum annual turnover of Rs.50 lakhs in previous three financial years ((2022-2023, 2023-2024 and 2024-2025).
b. The Bidder should have a minimum annual turnover of Rs 20 Crores in previous three financial years (2022-2023, 2023-2024 and 2024-2025).
c. For bidder applying under MSME the bidder should have a minimum annual turnover of Rs 1 Crores in previous three financial years (2021-2022, 2022-2023, 2023-2024)
d. The Bidder should have a positive net worth in previous three financial years (2022-2023, 2023-2024 and 2024-2025).

Bidder to provide applicable signed documents audited Balance sheet, Profit/Loss statement of the firm.

#	Financial Year	Total turnover (INR)	EBITA	Evidence	Pg. No. in current document
1	**2022-2023**			**E1.1.1**	
2	**2023-2024**			**E1.1.2**	
3	**2024-2025**			**E1.1.3**	

- E1: Kindly hyperlink the respective Evidence in above table
- E2: Kindly hyperlink the respective Evidence in above table
- …

Note: Bidders registered with NSIC/MSME, to provide valid NSIC/MSME Certificate.

2. **Appendix 2:**

   Copies of the Letter of acceptance (LoA) /work order/ purchase order/ contract/ completion certificate/ confirming relevant experience is to be shared in format mentioned below.

Evidence to be provided for handling assignments/ Services related to cyber security trainings/ Awareness Training sessions and content development in India during last three financial years [i.e. starting from 2019-2020 to 2023-2024].

#	Name of Organization	Date of P.O/Contract	Project Duration (in years)	Scope	Evidence	Pg. No. in current document
1	ABC	DD-MM-YYYY			E2.1	
2	DEF	DD-MM-YYYY			E2.2	
3						

- E1: Kindly hyperlink the respective Evidence in above table
- E2: Kindly hyperlink the respective Evidence in above table
- …

3. **Appendix 2:**
   Copies of the Letter of acceptance (LoA) /work order/ purchase order/ contract/ completion certificate/ confirming relevant experience during the last 05(five) years from the date of RFP.

   Provide detailed experience on handled assignments/ Services related to cyber security trainings/ Awareness Training sessions and content development to Regulator/BFSI/PSU/any University in India /any other large organization in India. Kindly add as many rows as required to highlight all relevant experiences.

#	Experience areas in handling training	Name of Organization	Date of P.O/Contract	Project Duration (in years)	Evidence (as stated above under appendix 3)	Pg. No. in current document
1		ABC	DD-MM-YYYY		E2.1.1	
2		DEF	DD-MM-YYYY		E2.2.1	
3						

- 2a.1: Kindly hyperlink the respective Evidence in above table
- 2a.2: Kindly hyperlink the respective Evidence in above table
- …

4. **Appendix 3:**

   Provide details of personnel. (Multiple certificate holders shall be counted once only)

#	Resource Name	Certification Name	Certification Number /ID	Certificate Issuance Date	Certificate Expiry Date	Evidence	Pg. No. in current document
1						E3.1	
2						E3.2	
3						E3.3	
4						E3.4	

Any Graduate with at least one certification out of CISA, OSCP, CISSP, C/PENT, CISM, CEH as per eligibility Criteria.

- E4.1: Kindly hyperlink the respective Evidence in above table
- E4.2: Kindly hyperlink the respective Evidence in above table
- …

5. Appendix 4:

The bidder should have LMS – learning management software either developed by them or partnership with respectable OEM to deliver the requirements of this RFP

#	Name of Organization	Date of P.O/Contract	Time taken for deployment	Project Duration (in years)	Scope	Evidence	Pg. No. in current document
1	**ABC**	**DD-MM-YYYY**				**E4.1**	
2	**DEF**	**DD-MM-YYYY**				**E4.2**	
3						**E4.3**	
4						**E4.4**	

- E5.1: Kindly hyperlink the respective Evidence in above table
- E5.2: Kindly hyperlink the respective Evidence in above table
- …

Authorized Signatory of the bidder
Name:
Designation:
Date:
Place:
Seal of the company

Executive Director (ERM) & CRO

भारतीय जीवन बीमा निगम
LIFE INSURANCE CORPORATION OF INDIA

Annexure D: Technical Scoring (Revised)

SN	Technical Evaluation Criteria – Parameters	Maximum Score
1.	The Bidder during the last 5 years' experience from the date of this RFP should be a knowledge partner for providing awareness sessions/trainings. • Above 5 Years->10 Marks • Above 3 Years to less than 5 Years ->7 Marks • Up to 3 years ->5 Marks (Supporting Document: Bidder should provide copies of the Letter of acceptance (LoA) /work order/ contract/ completion certificate/ confirmation email for relevant experience. The project completion date should be earlier than 5 years as on the date of this RFP) **Please refer Appendix-D1**	10
2.	The Bidder during the last 5 years from the date of this RFP should have worked as a knowledge partner as mentioned in RFP scope at organizations in PSU /Government /Private /BFSI Sector in India • Every reference ->2 Marks each Purchase order subject to maximum of 15 marks (Supporting Document: Bidder should provide copies of the Letter of acceptance (LoA) /work order/ contract/ completion certificate/ confirmation email for relevant experience. The project completion date should be during the last 5 years as on the date of this RFP) **Please refer Appendix-D1**	15
3.	The Bidder must have at least 5 personnel who have relevant experience to act as cyber security knowledge partner for content creation to impart awareness training as mentioned in the RFP scope. Valid certificates e.g. **CISA, OSCP, CISSP.C/PENT, CISM,CEH** are to be considered • 5 Resources -> 5 Marks • Every additional resource –>0.5 mark subject to maximum of 10 marks Multiple certificate holders shall be counted once only (Supporting Document: CVs of the concerned personnel with details of experience and qualification on company letter head duly signed by the authorized signatory of the bidder. Details to be provided- Name, Designation, Years of experience, Detailed description of experience, Qualifications and Certificates (if any). **Please refer Appendix-D2**	10
4.	Experience in imparting training on various aspects of cyber security as defined in this RFP. • Every referenced subject ->1 Mark each subject to maximum of 15 marks (Supporting Document: Bidder should provide copies of the Letter of acceptance (LoA)/work order/ contract/ completion certificate/ confirmation email for relevant experience. The project completion date should be within the last 5 years as on the date of this RFP) **Please refer Appendix-D1**	15
5.	The bidder shall be CERT-In empanelled as of date of this RFP **Please refer Appendix-D3**	5
6.	Experience in implementing Learning Management Solution • Every referenced subject ->2 Mark each subject to maximum of 15 marks (Supporting Document: Bidder should provide copies of the Letter of acceptance (LoA)/work order/ contract/ completion certificate/ confirmation email for relevant experience. The project completion date should be within the last 5 years as on the date of this RFP) **Please refer Appendix-D4**	15

SN	Technical Evaluation Criteria – Parameters	Maximum Score
7.	Learning management solution (LMS) compliance as per Appendix D6 on Compliance to LMS specification. Compliant to all technical specifications – 15 marks Non-compliant to any technical specification – 0 Marks **Please refer Appendix-D6**	15
8.	Technical presentation covering the following details (not a tentative list): • Skills and Experiences • Understanding of the objectives covered in the RFP. • Module aspects • Approach & methodology for conducting in-scope services. • Relevant Experience through successful project highlights of similar nature. • Availability of relevant skill set for execution of the project. **Please refer Appendix-D5**	15
Total		100

Appendices

1. **Appendix - D1**

Details of engagement as knowledge partner for providing awareness sessions/trainings at organizations in PSU /Government /Private /BFSI Sector/ University in India for last 5 years.Copies of the Letter of acceptance (LoA) /work order/ purchase order/ contract/ completion certificate/ confirming relevant experience. (To be shared in format mentioned below)

#	Experience areas in handling training	Name of Organization	Date of P.O/Contract	Project Duration (in years)	Evidence (as stated above under appendix 3)	Pg. No. in current document
1		**ABC**	**DD-MM-YYYY**			
2		**DEF**	**DD-MM-YYYY**			
3						

- A.1: Kindly hyperlink the respective Evidence in above table
- A.2: Kindly hyperlink the respective Evidence in above table
- …

2. **Appendix-D2:**

Provide details of personnel. (Multiple certificate holders shall be counted once only)
The Bidder must have at least 5 personnel who have relevant experience to act as cyber security knowledge partner for content creation to impart awareness training as mentioned in the RFP scope.

Valid certificates e.g. CISA, OSCP, CISSP.C/PENT, CISM, CEH are to be considered

#	Resource Name	Certification Name	Certification Number /ID	Certificate Issuance Date	Certificate Renewal Date	Evidence	Pg. No. in current document
1						**B.1**	
2						**B.2**	
3							

- B.1: Kindly hyperlink the respective Evidence in above table
- B.2: Kindly hyperlink the respective Evidence in above table
- …

3. Appendix-D3:

The bidder shall be CERT-In empaneled as of date of this RFP

#	Name of Organization	Date of empanelment	Certification Number /ID	Valid date	Next Renewal Date	Evidence	Pg. No. in current document
1						D.3.1	
2						D.3.2	
3							

- B.1: Kindly hyperlink the respective Evidence in above table
- B.2: Kindly hyperlink the respective Evidence in above table
- …

4. Appendix-D4:

The bidder should have LMS – learning management software either developed by them or partnership with respectable OEM to deliver the requirements of this RFP

#	Name of Organization	Date of P.O/Contract	Time taken for deployment	Project Duration (in years)	Scope	Evidence	Pg. No. in current document
1	ABC	DD-MM-YYYY				E5.1	
2	DEF	DD-MM-YYYY				E5.2	
3						E5.3	
						E5.4	

- E5.1: Kindly hyperlink the respective Evidence in above table
- E5.2: Kindly hyperlink the respective Evidence in above table
- …

5. Appendix D-5:

The bidder shall provide a technical presentation related to the in-scope services. The presentation date shall be conveyed to the bidders.

Scope of the Presentation (Tentative list):

- Skills and Experiences
- Understanding of the objectives covered in the RFP.
- Module aspects
- Approach & methodology for conducting in-scope services.
- Relevant Experience through successful project highlights of similar nature.
- Availability of relevant skill set for execution of the project.

- **Before the Presentation**: Share the soft copy (PDF) of the document with the relevant parties. This can be sent via email or shared through a file transfer platform.

- **After the Presentation**: Provide a signed hardcopy of the document. This can either be handed over physically or mailed, depending on the situation. Additionally, the signed PDF version must be shared to maintain an electronic copy of the signed document.

6. Appendix D-6 (Compliance to LMS)

Sl. No.	Description	Bidders Response	Compliance [Yes/No]
A.	**On-Premise**		
A. (i)	Name of the solution		
A. (ii)	Platform is deployable on private cloud instances of the organization integrated with PAM tool.		
A. (iii)	Please give hardware specification like RAM, CPU, HDD size with along with no. of servers required.		
A. (iv)	Please mention the details of enterprise wide software required for the activity which will be provided by the vendor in a separate sheet		
A. (v)	Name of OS other than RHEL to be provided by the vendor		
A. (vi)	Number of operating system other than RHEL and its version with number of licenses		
A. (vii)	Name of Database other than MySQL to be provided by the vendor		
A. (viii)	Number of Database other than MySQL and its version with number of licenses		
A. (ix)	Type of application - Web (both intranet & Internet) and Mobile application (.apk)		
A. (x)	Platform (Language-java,C#, Python etc.)		
A. (xi)	Software pre-requisites (.NET framework, IIS, IE, any other OS services, etc.)		
A. (xii)	Application to be accessible from both internet and intranet with high availability		
A. (xiii)	The infrastructure and application should be sized to take care the following: (d) at least 15 lakh agents with 5 % growth (e) 1 (one) lakh employees and (f) 10000 vendors Other details are given below: Concurrent Users : at least 20000 per second Maximum users: at least 50000 CPU utilization: not more than 60 % with a threshold of 80 %		
B.	**Useful Functionalities**		
B. (i)	Customization of Logo, Content, User and Subdomain - You can customize the logo and make changes accordingly, as far as for content and user you can update and provide extra information in the inbuilt Library.		
B. (ii)	Upload your own content (Up to 50GB) - There is inbuilt memory of 50 Gb where the super admin can upload the necessary and important data from their end. May be changed as per usuability.		
B. (iii)	Time shifting disabled (Forwarding Video) - Super admin can disabled the fast forwarding which leads to the given task being completed as its given time.		
B. (iv)	Lecture switching disabled till 100% completed - Super admin can also disabled the lecture switching, once the given lecture is completed (100%) then after the user can go to the next one.		

Sl. No.	Description	Bidders Response	Compliance [Yes/No]
B. (v)	Quiz within the course - There is also a quiz embedded in the course; once the lecture is completed users will be redirected to the quiz part. Quiz should also be part during presentation.		
B. (vi)	Custom Quiz Creation - Also create to own quiz and upload it to the course.		
B. (vii)	Auto Updating of the Library – Each month, we add new content to the tool based on current market trends and any new attacks discovered.		
B. (viii)	Adaptive Learning - Not just one size fits all. Ascertain which user is weak in which area of security awareness and sequence the training in that order, in a personalized manner individually.		
B. (ix)	Track learning progress by department/job title/location/team/group and Definitely dynamic groups		
B. (x)	Integration with LIC's Applications (Employees, agents, customers and vendors) i.e. Intranet of LIC, Customer portal, Agents ports, licindia.in, HRMS, concurrencia etc.		
B. (xi)	The solution can be configured to automatically enroll and engage (send them welcome/what-to-do email) to newly added users		
B. (xii)	All internal communication like advisories should have "I Acknowledge" (Sign-off) feature, such that users can confirm that they have read and understood/acknowledged the advisories sent to them.		
B. (xiii)	Platform should have support for publishing organization policies and user should have option to accept the policy.		
B. (xiv)	Platform should have a library of quiz questions and ability to add new and relevant questions to the library.		
B. (xv)	Platform should have a library of quiz questions and ability to add new and relevant questions to the library		
B. (xiv)	Ability to create dynamic lists for re-targetting or reporting to management on Users that did an action, but DID NOT DO another follow-on action. Example: Opened Simulation> NOT compromised, and NOT reported". This should be available for campaigns over a period of time, and not just for single campaigns.		
B. (xv)	Exhaustive library of announcements, Wallpapers, Screensavers, tips and tricks, infographics, posters, banners etc. in English, Hindi etc.		
C.	**Learning Types**		
C. (i)	Content Library - The inbuilt Content library should have the capability to contain at least 300 modules which include various types of Lecture Video, Webinars , question bank etc.		
C. (ii)	Regional Language – Content are already available with different regional languages like English, Hindi.		
C. (iii)	Certification after course completion - Once a user completed the course assigned to him/her, they will automatically get the Certification of course completion.		
D.	**Reporting and Tracking**		
D. (i)	Employees' progress track record - Super admin can track the progress of users regarding the assigned course.		
D. (ii)	Course-wise reporting - Super admin can track the users regarding the duration of video, departments and also the active learners.		

Sl. No.	Description	Bidders Response	Compliance [Yes/No]
D. (iii)	The Super Admin can track the number of employees who have completed watching a lecture as well as those who have discontinued or dropped out		
D. (iv)	Stats on best performing employees - Statistics of best performing employees can be seen in the reporting section.		
D. (v)	User Inactivity Tracking - User inactivity can also be tracked by analyzing the mouse movement and keyboard activity. After being inactive for 10 minutes, the user should be logged out of the module		
D. (vi)	Background Watch Disabled (Video) - When an employee switches the tab or minimizes it, the lecture video will be automatically paused.		
D. (vii)	Failure Reminder - When an employee fails the course, a remainder will be sent to the higher authority, or the manager assigned to him/her.		
D. (viii)	Escalation Reminder – After the multiple reminders if an employee still fails to attempt or complete the course the admin can send the reminder to the Team Manger directly giving them the status and analytics of their team.		
D. (ix)	Leaderboard – You can also view information about the top performers in a campaign, including who completed their training first and achieved the highest score.		
D. (x)	Provision should be there regarding completion cases through internet/Intranet/mobile App along with duration taken, no of attempts etc.		
E.	**Content Management**		
E. (i)	Upload custom files - Super admin can upload PDF, PPT documents in the LMS and can add in a course for a user to preview and utilize.		
E. (ii)	Service provider must provide access to a team of graphic designers, content writers, illustrators, stock video footage, voiceover artists, hackers with real world knowledge to generate original content for our organization, based on our brand guidelines and policies		
E. (iii)	Service provider must ensure access to security awareness training managers and hackers to consult for the creation of announcements, infographics, posters, standees, screensavers to match our brand guidelines.		
E. (iv)	Create on-boarding and welcome videos to meet all our information security policies		
E. (v)	Create a mascot to make all information security content visually identifiable. Operate it like a brand mascot for the information security team. All communications will include this mascot.		
E. (vi)	Custom Videos to be created on Breach and News triggered threats uncovered recently. Example: Samsung employees used ChatGPT, and confidential data was uploaded and leaked. We will alert our users of this pertinent threat as soon as this news breaks.		
E. (vii)	Create custom videos to drive home cyber awareness		
E. (viii)	Create a custom program for Cyber Security Awareness Month (typically in October) to drive user awareness in a concerted campaign during that entire period		

Sl. No.	Description	Bidders Response	Compliance [Yes/No]
E. (ix)	Deliver custom and branded content to users with a 360 degree surround to create stickiness with workshops, offline posters, danglers, standees for offices and online content like emails, infographics, games, quizzes, contests, actions to be taken in receipt of phishing mails etc.		
E. (x)	Undertake content collaborations featuring senior leadership from across our organization, to ensure that there is a feeling of joint ownership from Unit and Department heads with them being featured in that content		
E. (xi)	Release periodic Newsletters for END USERS from the CISO office to ensure that all users are kept up to date on specific breaches within our industry and what end users can do to protect themselves. English, Hindi etc.		
E. (xii)	Release periodic Newsletters for SENIOR MANAGEMENT to update them on cyber news and events pertinent to senior management.		
E. (xiii)	The content should be updated as and when necessary in line with the terms and conditions of RFP and applicable mandates.		
F.	**End User Portal**		
F. (i)	Users can login to their own profile using AD/SSO integration along with physical Biometric access for employees, OTP for others. For external login of employees OTP will be enabled. Provision should be there to use Google authenticator for all cases.		
F. (ii)	Users can login to their own profile using their Email address only, and a unique link gets delivered to their email with validity of 30 minutes. This can be a password less mechanism i.e like a unique link delivered to their own email.		
F. (iii)	Undertake their training assigned to them, as well as undertake optional courses for gaining further points and increasing their awareness		
F. (iv)	Users should be able to see their performance on their engagement with announcements, advisories, training, complete courses, see their actions, their points (gained and lost), their badges, their certificates, leaderboard by team, department, and organization wide.		
F. (v)	See and act upon their risk score, and their risk score history/trend to track their risk rating over a period of time		
F. (vi)	End users should be able to see all the latest advisories, notifications, announcements, cyber news released by the CISO office in one cyber inbox. Emails/Messages may be scattered but there should be one place to read all things related to cyber security from the CISOs office (Just like a bank sends emails etc. but notifications are available on the banking website in one inbox in one place.)		
F. (vii)	End users should be able to download their personalized certificates, badges, levels achieved etc.		
F. (viii)	Manager's Portal: Managers can add/modify/delete users and also eligible for bulk upload using .csv file based on authorization with segregation of duties.		
F. (ix)	Managers can view the Leaderboard position, Risk Score, & Announcement performance of their direct teams, sub-teams and direct and indirect reportees.		

Sl. No.	Description	Bidders Response	Compliance [Yes/No]
F. (x)	Manager's portal must allow managers to easily identify weak performers within their direct reports, as well as within the sub-teams under their reportees.		
F. (xi)	Assign Skills to Courses - There are various skills which can be auto assigned to a user once they complete a course.		
F. (xii)	Create new Skills - The super admin can also create new skills and assign on courses.		
F. (xiii)	Manage Skills - The super admin can also edit the existing Skills.		
G.	**Roles**		
G. (i)	Define roles - A super admin can define various user profiles for low level access to administrators. Hierarchical visibility of users data and status should be available in the categorization of Satellite office-Branch office-Divisional Office-Zonal Office-Central Office		
G. (ii)	Role Assignment - A super admin can assign various user profiles for low level access to administrators.		
G. (iii)	Teams and Team Hierarchies - Different teams and hierarchies can be defined for Employees/Users.		
H.	**Accounts**		
H. (i)	No Signup Required - With a magic link users can login to the dashboard without typing any credentials (based on OTP by checking the mobile no and email id)		
H. (ii)	Add a new User - There is functionality available to add users using Active Directory and CSV based file uploads.		
H. (iii)	Archive Users - There is an option to archive users who have left the organization, or the accounts have been deactivated.		
H. (iv)	Bulk User Actions - There are bulk actions which can be taken based on user groups		
H. (v)	Access Management - Two factor authentications (both biometric access and OTP access) should be enabled for any administrative/user activities.		
I	**Security**		
I. (i)	IP Blocker - There is platform-based security available in terms of IP level blocking for dashboard access.		
I. (ii)	Strong Password parameters - Strong password parameters need to be enabled.		
J	**Assessment**		
J. (i)	Default Assessment - There are various assessments available which can be assigned to the users.		
J. (ii)	Customizable Assessment - The assessment are fully customizable as per the requirement to add your own questions		
J. (iii)	Customizable Certificates - The certificates are posted to users after they complete a course which can be customized for name, logo, design & Signature.		
K.	**Training and awareness**		
K. (i)	Fully featured LMS with capability to assign and track training with an extensive library of cyber security content covering core topics + periodic updates to that content + With content in English, Hindi etc.		
K. (ii)	Ability to train with Microsoft Teams as a channel of communication: For training assignments, reminders, cyber security announcements, upcoming events, cyber security		

Sl. No.	Description	Bidders Response	Compliance [Yes/No]
	inforgraphics using API based integration with MS Teams		
K. (iii)	Auto enrolment of new employees through AD/HRMS/Others. The solution can be configured to automatically enroll and engage (send them welcome/what-to-do email) to newly added users		
K. (iv)	Platform should support Roles Based Access Control, i.e. Super Admin, Admin, Report Viewer, Training Assignment Manager, other Managerial roles etc.		
L.	**Managed Services**		
L. (i)	Strategy, Development & Planning-Dedicated Managed Services SPOC to design and implement specific security awareness and training program		
L. (ii)	Continuous Training- Assess, Educate, Reinforce & Measure the learning program to minimize the phishing assaults and malware infections successfully		
L. (iii)	Collaborative Planning- Managed Services team to identify reporting requirements prior to execution to ensure important attributes are measured and included in reporting		
L. (iv)	Continuous Assessment- Periodic cadences to review results, share insights and solicit feedback to make necessary adjustments to training plan		
L. (v)	Quantitative Objective Driven- To identify the end objective of improving awareness and preparedness in the organization by percentages		
M.	**Integration/Orchestration**		
M. (i)	Platform should support SSO and secure AD integration/ AD Sync along with two factor authentication.		
M. (ii)	APIs should be available for integration with other business systems/Power BI etc. to customize and obtain reports and data points		
M. (iii)	Platform should be capable of integrating with multiple SIEM tools like Splunk, QRadar etc., SOAR and UEBA Platforms, SEGs, Proxies, Sandboxes, DLP, ITSM, IAM, PAM tool etc.		
N.	**Enforcement**		
N. (i)	Positive Enforcement-Badges, Certificates, Coupons, Awards enablement and appreciation on the portal.		
O.	**Compliances to various mandates**		
O. (i)	The module should be compliant to various mandates applicable for LIC e.g. IRDAI, GOI like Cert-In, DFS, NCIIPC etc.		
O. (ii)	The observations identified during technical audit and process audit must be closed within 7 working days.		
O. (iii)	The server, database, application should be hardened by following various standards such as NIST, CIS, OWASP top 10 as well as best practices as applicable in line with various applicable mandates.		
O. (iv)	SOP should be prepared for all activities and administrator in clarity with screenshots.		
P.	**Status update**		
P. (i)	Provision should be there for status update of trainings conducted along with no. of trainees successfully completed the activities.		
P. (ii)	Categorized Proper reconciliation of trainees status e.g. pass, fail, yet to be appeared etc.		

Sl. No.	Description	Bidders Response	Compliance [Yes/No]
Q.	**Risk Scoring**		
Q. (i)	Each employee should get a Human Cyber Risk Score based on key criteria: their security behavior + their training + it must factor their job role, privileged access to ensure that the score for risk is appropriately measured		
Q. (ii)	Leaderboard to measure and mitigate risk at each department, location, org wide level.		
Q. (iii)	Risk scoring to be visible to individual users (end-user portal) and their Managers (Manager's portal) or Department Head, Unit Head, Admin - with strict role based access control. Manager can only see reportee reports. This feature should be available to switch on and off, as the need may be from time to time.		
Q. (iv)	Representation of risk scoring to be done like a risk meter, with historic risk scoring shown in a graph format to track progress or deterioration		

Note:

• Bidder must comply with the above-mentioned criteria. Non-compliance to any of the criteria may entail rejection of the bid. LIC reserves the right to verify/evaluate the claims made by the bidder independently. Any misrepresentation will entail rejection of the offer.

• Evidence to be submitted for each criteria should be part of the same response document. Proper naming and indexing should be done to avoid any ambiguity.

• The bidder who successfully qualifies in the eligibility criteria, only their technical bids will be subsequently opened for further evaluation.

Authorized Signatory of the bidder
Name:
Designation:
Date:
Place:
Seal of the company

Executive Director (ERM) & CRO

Addendum-2: Mile stone based payments included in Section G

Additional Milestone based terms and conditions related to payment

Milestone based payments to be released based on performance

Implementation of LMS Platform (only in 1st year)	Maximum 20% of the contract value
Creation and Upload of contents (To be covered for all 5 years)	Maximum 15% of the contract value
Conduct of Annual Training and Quiz (To be covered for all 5 years)	Maximum 40% of total contract value
On-Site Trainer (Full Time to be available in LIC premises) (To be covered for all 5 years)	Maximum 15% of the Contract value
On-site System Administrator (Full Time to be available in LIC premises) (To be covered for all 5 years)	Maximum 10% of the contract value
Annual Maintenance charges including change management (To be covered for all 4 years after one year of GO-Live of the project)	Maximum 10% of the contract value

Detailed Milestones

Milestones to be completed	Details of activities	Payments to be released	Bifurcation of payments
Implementation of LMS Platform (First Year Cost)	1. Licenses 2. Installation 3. Fine tuning as per LIC's requirement 4. Testing in UAT environment 5. GO-LIVE of the platform 6. Integration with PAM, IAM, SIEM, DAM, Intranet portal of LIC and HRMS module	Maximum 20% of the contract value	• 60% on installation and Testing of UAT and sharing of license certificate • 30% upon GO-Live of the project • 10% upon post six months of Go Live of the Module completion
Creation and upload of contents (Cost to be distributed across 5 years	1. Creation of all contents in Hindi and English Medium 2. Audio, video (all formats to be provided and uploaded) 3. Implementation of Access control 4. Implementation of Role Based Access to the contents of the module 5. Annual updation of contents	Maximum 15 % of the contract value	Not Applicable
Conduct of Annual Training and Quiz (Cost to be distributed across 5 years	Approval of Webinars, Audio, Presentations, SMS, Emails, Flyers, brochures, social media coverage etc. covering employees, agents and vendors and ensure its upload	Maximum 40 % of total contract value	Not more than 40 %
	Approval of SMS, small video, SMS, Emails, social media coverage etc. for customers		Not more than 10 %
	Cyber Jagrookta Diwas		Not more than 5 %
	Quiz and Assessment		Not more than 20 %
	Tabletop Exercises		Not more than 5 %
	Feedback (Above 3.0 out of 5)		Not more than 5 %

Milestones to be completed	Details of activities	Payments to be released	Bifurcation of payments
On-Site Trainer (Full Time to be available in LIC premises) (Cost to be distributed across 5 years	Daily attendance, Imparting Training to all sections, Preparation of training schedule, Tracking, monitoring and review of user participation, liasioning with stakeholders for completion of training and quiz, achieve feedback, SLA monitoring	Minimum 15 % of the Contract value	Not Applicable
On-site System Administrator (Cost to be distributed across 5 years	Daily attendance, achieve high availability of 99.999 %, Support in implementation of various patches related to OS, Database and application, day-to-day operation, managing changes, tracking implementation of changes as suggested by LIC, feedback, SLA monitoring	Minimum 10 % of the contract value	Not Applicable
Annual Maintenance charges including change management (Cost to be distributed across 4 years		Minimum 10 % of the contract value	Not Applicable

Executive Director (ERM) & CRO