On-boarding Cyber Security Knowledge Partners for Awareness Training sessions for Employees, Agents, Vendors, Customers and other Stakeholders
Technical Bid Document

CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June 2025

Enter Bidder's Name ____________________

Instructions

1 . Bidder has to compulsorily comply for all items.
2 . Excel Cells where Bidder has to input values, are unlocked.
3 . Print outs of all sheets are required to be duly signed, stamped and submitted.
4 . Reference may be made to the RFP for details.
5 . The bidder can provide the quotes only in blue 🟦 coloured cells.

Bidder's name	0

On-boarding Cyber Security Knowledge Partners for Awareness Training sessions for Employees, Agents, Vendors, Customers and other Stakeholders
Technical Bid Document
CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June 2025

Annexure – D: Technical Scoring - Appendix D1 - Letter of acceptance (LoA) /work order/ purchase order/ contract/ completion certificate/ confirming relevant experience during last Five financial years
[i.e. 2020-2021, 2021-2022, 2022-2023, 2023-2024 and 2024-2025].

Name of Organization	Date of P.O/Contract	Project Duration in years	Value of P.O (INR)	Scope	Evidence	Reference Page No.

Name of Organization	Date of P.O/Contract	Project Duration in years	Value of P.O (INR)	Scope	Evidence	Reference Page No.

For agreements as evidence, certified copy of the 1st page and last page of each agreement along with the page containing the required evidence should be enclosed as hardcopy and Scanned copy of complete agreement should be provided in the CD.

This is to cerify that no correction / modifications have been done in this sheet and hardcopy matches exactly with softcopy that is being submitted

Signature of Bidder/Bidder's Representative

Stamp and Seal

Date:

Bidder's name	0

On-boarding Cyber Security Knowledge Partners for Awareness Training sessions for Employees, Agents, Vendors, Customers and other Stakeholders
CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June 2025

Annexure – D: Technical Scoring - Appendix D2 - Provide details of personnel.
(Multiple certificate holders shall be counted only once)

#	Name of Resource	Name of Certification	Certification ID/No.	Certificate issuance date	Certificate Renewal Date	Reference Page No.(Copy of certificate
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						
26						
27						
28						
29						
30						
31						
32						
33						
34						

35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						

For agreements as evidence, certified copy of the 1st page and last page of each agreement along with the page containing the required evidence should be enclosed as hardcopy and Scanned copy of complete agreement should be provided in the CD.

This is to cerify that no correction / modifications have been done in this sheet and hardcopy matches exactly with softcopy that is being submitted

Signature of Bidder/Bidder's Representative **Stamp and Seal of the Company** **Date**

Bidder's name	**0**

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

Technical Bid Document

CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June 2025

Annexure – D: Eligibility Criteria - Appendix D3 - Cert-In Empanelment

Sl. No.	Name of Organization	Date of empanelment	Certification Number /ID	Valid date	Next Renewal Date	Evidence	Pg. No. in current document

For agreements as evidence, certified copy of the 1st page and last page of each agreement along with the page containing the required evidence should be enclosed as hardcopy and Scanned copy of complete agreement should be provided in the CD.

This is to cerify that no correction / modifications have been done in this sheet and hardcopy matches exactly with softcopy that is being submitted

Signature of Bidder/Bidder's Representative

Stamp and Seal of the Company

Bidder's name	**0**

On-boarding Cyber Security Knowledge Partners for Awareness Training sessions for Employees, Agents, Vendors, Customers and other Stakeholders
Technical Bid Document

CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June 2025

Annexure – D: Technical Scoring - Appendix D4 - Letter of acceptance (LoA) /work order/ purchase order/ contract/ completion certificate/ confirming relevant experience during last Five financial years
[i.e. 2020-2021, 2021-2022, 2022-2023, 2023-2024 and 2024-2025] for LMS

#	Name of Organization	Date of P.O/Contract	Time taken for deployment in months	Project Duration (in years)	Scope	Evidence	Pg. No. in current document

For agreements as evidence, certified copy of the 1st page and last page of each agreement along with the page containing the required evidence should be enclosed as hardcopy and Scanned copy of complete agreement should be provided in the CD.

This is to cerify that no correction / modifications have been done in this sheet and hardcopy matches exactly with softcopy that is being submitted

Signature of Bidder/Bidder's Representative

Stamp and Seal

Bidder's name	0

On-boarding Cyber Security Knowledge Partners for Awareness Training sessions for Employees, Agents, Vendors, Customers and other Stakeholders
CO-ERM-IT-CSD-2025-2026/IS Awareness dated 18th June 2025
Annexure – D: Technical Scoring - Appendix D6 - Compliance to LMS Specifications

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
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:				
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.				
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.				
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 - You can also create your 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)				
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" 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)	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. (xvi)	Ability to take individual action on dynamic groups like Phished X times in X Months, Opened but not reported in X months, Phished but not started reporting in X months, etc.				
B. (xvii)	Personalized feedback emails to users on their actions. Opened but not clicked. Clicked but not phished. Phished but not reported. Opened but not reported etc.				
B. (xviii)	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.				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
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.				
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 analysing 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 (to be changed regularly)**				
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 organisation, 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 relevant phishing simulation scenarios, 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				
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, phishing simulations 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				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
F. (iv)	Users should be able to see their performance on phishing simulations, their engagement with announcements, advisories, training, complete courses, see their actions, their points (gained and lost), their badges, their certificates, the leaderboard by team, department, and organisation 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, Phishing Performance & Announcement performance of their direct teams, sub-teams and direct and indirect reportees.				
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.				
H. (vi)	Biometric access should be enabled for employees to access LMS and 2FA for others.				
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 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				

Sl. No.	Description	Bidders Response	Compliance [Yes/No]	Evidence, if any	Pg. No. in current document
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.				
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				

For agreements as evidence, certified copy of the 1st page and last page of each agreement along with the page containing the required evidence should be enclosed as hardcopy and Scanned copy of complete agreement should be provided in the CD.

This is to cerify that no correction / modifications have been done in this sheet and hardcopy matches exactly with softcopy that is being submitted

Signature of Bidder/Bidder's Representative

Stamp and Seal