

Terms of Reference

Engagement of an External Training Service Provider for Conducting Cybersecurity Capacity Building Programs

(CERT/GOSL/CON/CQS/2026/12)

1. Background

Sri Lanka Computer Emergency Readiness Team (Sri Lanka CERT) is the national focal point for cybersecurity in Sri Lanka and is responsible for strengthening the nation's cyber resilience through incident response, cyber threat monitoring, cybersecurity policy implementation, awareness creation, capacity building, and stakeholder collaboration.

As part of the implementation of the National Information and Cyber Security Policy and the Government's digital transformation initiatives, Sri Lanka CERT conducts cybersecurity awareness and capacity building programmes targeting government ministries, departments, provincial councils, district secretariats, statutory bodies, and other public sector organizations.

In addition, Sri Lanka CERT has recognized the need to significantly expand cybersecurity awareness and capacity building programmes throughout the country to improve the cyber resilience of public sector institutions.

Over the past several years, Sri Lanka CERT has successfully delivered numerous cybersecurity awareness programmes using its internal technical experts. However, with the rapid increase in national cybersecurity responsibilities, including cybersecurity monitoring, incident response, threat intelligence, digital forensics, policy implementation, technical advisory services, and support for Critical National Information Infrastructure (CNII), the organization now faces increasing limitations in allocating sufficient internal resources to conduct large-scale awareness programmes across the country.

To address this challenge while maintaining the quality and consistency of awareness programmes, Sri Lanka CERT intends to engage a qualified and experienced external training service provider to deliver standardized cybersecurity capacity building programmes under the technical guidance and supervision of Sri Lanka CERT.

The selected service provider shall work closely with Sri Lanka CERT to organize, coordinate, and conduct cybersecurity awareness programmes in selected provinces and districts while ensuring that all training materials, delivery methodologies, and programme outcomes comply with the standards and requirements established by Sri Lanka CERT.

2. Objectives

The overall objective of this assignment is to engage a competent external training service provider to support Sri Lanka CERT in delivering standardized cybersecurity capacity building programmes for government sector officials throughout Sri Lanka (9 Provincial Councils).

The specific objectives are to:

- a. Conduct high-quality cybersecurity awareness and capacity building programmes for approximately 2,000 government officials across selected ministries, departments, provincial councils, district secretariats, and other government institutions.
- b. Expand the geographical coverage of cybersecurity awareness programmes by conducting training programmes in selected provinces and districts across the country.
- c. Deliver standardized training programmes using training materials, technical content, and awareness methodologies approved by Sri Lanka CERT.
- d. Enhance the cybersecurity awareness, cyber hygiene practices, and understanding of cyber threats among government officials.
- e. Ensure consistent quality, delivery standards, participant engagement, and learning outcomes across all awareness programmes.
- f. Provide comprehensive programme coordination, participant management, reporting, evaluation, and documentation for each training programme conducted.
- g. Support Sri Lanka CERT in achieving national cybersecurity capacity building objectives while enabling its internal technical staff to focus on core operational cybersecurity functions.

3. Scope of Work

The selected Training Service Provider shall provide end-to-end services for planning, coordinating, organizing, delivering, monitoring, and reporting cybersecurity capacity building programmes under the overall supervision of Sri Lanka CERT.

The scope of work shall include, but not be limited to, the following activities.

3.1 Programme Planning and Coordination

The service provider shall:

- Develop an overall implementation plan for all assigned training programmes.
- Coordinate with Sri Lanka CERT and participating government institutions regarding programme schedules, participant nominations, venue arrangements, and logistics.
- Maintain an annual/master training schedule in consultation with Sri Lanka CERT.
- Ensure timely communication with participating organizations before each programme.

3.2 Training Programme Delivery

The service provider shall conduct approximately 40 cybersecurity awareness programmes targeting approximately 2,000 government officials (minimum 50 participants per programme) at locations (9 Provincial Councils) identified by Sri Lanka CERT.

Training programmes shall include topics such as:

- Current Cyber Threat Landscape:
 - Current cyber threat landscape

- National cyber incidents
 - Global cyber trends
 - Emerging cyber threats
- Cyber Hygiene Best Practices:
 - Password security
 - Multi-factor Authentication
 - Safe Internet Usage
 - Email Security
 - Web Browsing Safety
 - Device Security
 - Mobile Security
- Password and Authentication Security
- Phishing and Social Engineering
 - Phishing
 - Spear Phishing
 - Business Email Compromise
 - QR Code Scams
 - Voice Phishing
 - SMS Scams
- Email Security
- Internet and Social Media Safety
- Malware and Ransomware Awareness
 - Ransomware
 - Spyware
 - Trojans
 - Data Theft
 - Malware Prevention
- Mobile Device Security
- Safe Use of AI and Emerging Technologies
- Data Protection and Privacy
- Government Information and Cyber Security Policy
 - Government Information and Cyber Security Policy
 - Roles and Responsibilities
 - Incident Reporting
 - Cyber Risk Management
 - Information Classification
 - Secure Handling of Government Information
- Incident Reporting Procedures
- Practical Demonstrations and Real-world Case Studies

- Other topics identified by Sri Lanka CERT.
 - Personal Data Protection
 - Privacy Principles
 - Secure Data Handling
 - Safe Information Sharing
 - Artificial Intelligence
 - Cloud Security
 - Internet of Things
 - Digital Identity
 - Emerging Cyber Risks

The exact programme content shall be determined and approved by Sri Lanka CERT. Sri Lanka CERT reserves the right to modify or add training topics at any time during the contract period.

3.3 Training Materials

The service provider shall:

- Design, develop, and maintain all required training materials.
- Prepare presentation slides, facilitator guides, participant handbooks, practical exercises, quizzes, and evaluation forms.
- Obtain written approval from Sri Lanka CERT prior to using any training material.
- Revise training materials whenever requested by Sri Lanka CERT.

3.4 Programme Administration

The service provider shall:

- Handle participant registration.
- Prepare attendance records.
- Manage participant communications.
- Coordinate venue logistics where applicable.
- Provide required stationery and printed training materials.
- Print and distribute certificates approved by Sri Lanka CERT.
- Maintain participant databases.

3.5 Monitoring and Quality Assurance

The service provider shall:

- Ensure that all programmes are delivered according to the quality standards established by Sri Lanka CERT.
- Conduct participant feedback surveys.

- Administer pre-training and post-training evaluations where applicable.
- Maintain programme quality records.
- Implement corrective actions based on participant feedback and Sri Lanka CERT observations.

3.6 Reporting

The service provider shall submit programme reports including:

- Programme summary.
- Participant attendance.
- Photographic evidence.
- Participant evaluation results.
- Feedback analysis.
- Issues encountered.
- Recommendations.
- Monthly progress reports.
- Final project completion report.

All reports shall be submitted in both editable and PDF formats.

3.7 Technical Specifications / Statement of Requirements

The selected Service Provider shall provide a complete end-to-end service for the planning, coordination, management, and delivery of Cybersecurity Capacity Building Programmes in accordance with the requirements specified by Sri Lanka CERT.

The Service Provider shall be responsible for providing, at a minimum, the following services.

No.	Requirement	Minimum Requirement
1	Project Management	Assign a dedicated Project Manager as the single point of contact throughout the assignment.
2	Programme Planning	Develop a detailed implementation plan and annual programme schedule in consultation with Sri Lanka CERT.
3	Coordination	Coordinate with Ministries, Departments, Provincial Councils, District Secretariats, and other Government institutions before each programme.
4	Trainers	Provide qualified cybersecurity trainers approved by Sri Lanka CERT.
5	Language	Deliver programmes in Sinhala, Tamil and/or English as instructed by Sri Lanka CERT.
6	Training Materials	Develop presentation slides, facilitator guides, participant handbooks, exercises, and awareness materials approved by Sri Lanka CERT.

No.	Requirement	Minimum Requirement
7	Participant Management	Registration, attendance verification, participant database, and communication.
8	Programme Delivery	Conduct approximately 40 awareness programmes for approximately 2,000 participants.
9	Assessments	Conduct pre-training and post-training assessments where applicable.
10	Feedback	Collect participant feedback using approved evaluation forms.
11	Certificates	Print and distribute certificates approved by Sri Lanka CERT.
12	Photography	Capture photographs during each programme and submit them with the completion report.
13	Reporting	Submit programme reports, monthly reports, and final completion report.
14	Quality Assurance	Maintain internal quality assurance procedures throughout the assignment.
15	Knowledge Transfer	Submit all editable training materials, source files, templates, and supporting documents to Sri Lanka CERT.

3.8 Minimum Technical Requirements for Each Awareness Programme.

Each awareness programme shall comply with the following minimum standards unless otherwise instructed by Sri Lanka CERT.

Item	Requirement
Programme Duration	Approximately 4–6 Hours (or as instructed by Sri Lanka CERT)
Participants	Minimum 50 participants
Delivery Mode	Physical / Online / Hybrid
Venue	As identified by Sri Lanka CERT
Language	Sinhala / Tamil / English
Attendance	Mandatory attendance recording
Assessment	Pre/Post assessment where applicable
Feedback	Mandatory participant evaluation
Certificate	Certificate of Participation
Report	Programme Completion Report

3.9 Programme Deliverables for Each Session

For every programme conducted, the Service Provider shall submit the following.

Before the Programme

- Confirmed participant list
- Programme agenda
- Trainer details
- Presentation materials
- Logistics confirmation

During the Programme

- Registration
- Attendance
- Programme coordination
- Photography
- Evaluation
- Certificate preparation

After the Programme

- Attendance sheet
- Programme report
- Participant feedback
- Assessment summary
- Photographs
- Lessons learned
- Issues encountered
- Recommendations

All reports shall be submitted within five (05) working days after completion of each programme.

3.10 Service Level Requirements (SLA)

The Service Provider shall comply with the following minimum service levels.

Requirement	Service Level
Programme cancellation	Minimum 5 working days' notice
Replacement trainer	Within 24 hours of notification
Monthly report	Within 5 working days after month-end
Programme report	Within 5 working days

Requirement	Service Level
Final report	Within 15 working days after contract completion
Response to Sri Lanka CERT	Within 1 working day
Revision of deliverables	Within 5 working days unless otherwise agreed

3.11 Quality Standards

The Service Provider shall ensure:

- Consistent delivery across all locations.
- Trainers are professionally dressed and conduct themselves appropriately.
- High-quality presentation materials.
- Effective participant engagement.
- Accurate attendance records.
- Proper branding using Sri Lanka CERT-approved templates.
- No unauthorized use of Sri Lanka CERT logos or materials.

4. Programme Requirements

The Service Provider shall ensure that all programmes meet the following minimum requirements.

- **Number of Programmes**

Approximately 40 awareness programmes shall be conducted during the contract period.

- **Target Audience**

Approximately 2,000 government officials representing ministries, departments, provincial councils, district secretariats, statutory bodies and other government institutions.

- **Programme Size**

Each programme shall accommodate not less than 50 participants, unless otherwise approved by Sri Lanka CERT.

- **Duration**

Unless otherwise instructed, each awareness programme shall be conducted as a one day programme (approximately 4 - 6 hours).

- **Mode of Delivery**

Training programmes may be conducted:

- Physical
- Online
- Hybrid

depending on the requirements of Sri Lanka CERT.

- **Geographic Coverage**

Training programmes shall be conducted throughout Sri Lanka at locations (9 Provincial Councils) identified by Sri Lanka CERT. The Service Provider shall be capable of deploying training teams to all provinces and districts when required

5. Deliverables and Payment Schedule

The selected Training Service Provider shall successfully complete and submit the following deliverables to the satisfaction of Sri Lanka CERT.

Deliverable	Description	Timeline
D1	Inception Report including implementation methodology, work plan, programme schedule, communication plan and resource allocation	Within 10 working days from contract signing
D2	Training Materials Package including presentations, facilitator guide, participant handbook, practical exercises, evaluation forms and certificate design	Within 20 working days
D3	Delivery of Cybersecurity Capacity Building Programmes	Throughout the contract period
D4	Programme Completion Reports (for each programme conducted)	Within 5 working days after each programme
D5	Monthly Progress Report	Monthly
D6	Final Completion Report including overall statistics, lessons learned, recommendations and all supporting documents. The Final Completion Report shall include, but not be limited to: • Executive Summary • Number of programmes conducted • Number of participants trained • Institution-wise participation • Province/District-wise coverage • Attendance summaries • Participant feedback analysis • Training evaluation results • Photographic documentation • Challenges encountered • Recommendations for future programmes • Soft copies of all training materials	Within 15 days after completion of the assignment

Deliverable	Description	Timeline
	Soft copies of attendance sheets and evaluation results	

Deliverable	Payment
Submission and approval of Inception Report and Training Materials	20%
Completion of approximately 50% of assigned programmes with accepted reports	30%
Completion of all assigned programmes	30%
Submission and acceptance of Final Completion Report and all project documents	20%

Payments shall only be processed after:

- Acceptance of deliverables.
- Submission of invoices.
- Submission of all required reports.
- Certification by the Project Manager appointed by Sri Lanka CERT.

5. Timeline and Duration

The expected duration of this assignment shall be Six (06) months from the date of signing the contract, unless otherwise agreed by Sri Lanka CERT. The contract may be extended based on performance, availability of funds, and operational requirements.

6. Qualifications and Experience

The Service Provider shall be a legally registered organization with proven expertise in designing and delivering cybersecurity awareness, capacity building, or professional training programmes.

The Service Provider shall demonstrate the following minimum qualifications and experience:

6.1 Organizational Requirements

The Service Provider shall:

- Be a legally registered business entity in Sri Lanka.
- Have been in operation for a minimum of five (05) years.
- Have experience in conducting large-scale training programmes for Government, public sector organizations, private sector organizations, universities, or international agencies.
- Demonstrate sound financial and organizational capacity to undertake this assignment.

- e. Have adequate administrative and project management resources to coordinate nationwide training programmes.

6.2 Technical Experience

The Service Provider shall have demonstrated experience in:

- Cybersecurity/ IT security awareness programmes
- Information security capacity building
- Cybersecurity professional training
- Information security governance
- Digital safety awareness
- Secure use of emerging technologies
- Development of training materials and awareness resources

Preference will be given to organizations that have successfully completed similar assignments for Government institutions, national level organizations or corporate reputed entities.

6.3 Key Personnel Requirements

The Service Provider shall nominate the following minimum key personnel.

Project Manager

Minimum Qualifications:

- Bachelor's degree in information technology, Computer Science, Information Systems, Cyber Security or related field.

Minimum Experience:

- Minimum five (05) years of project coordination or programme management experience.

Responsibilities:

- Overall coordination of the assignment
- Liaison with Sri Lanka CERT
- Programme scheduling
- Quality management
- Reporting

Lead Cybersecurity Trainer(s)

Minimum Qualifications:

- Bachelor's degree in information technology, Computer Science, Cyber Security or related discipline.

Professional certifications such as one or more of the following shall be considered an added advantage:

- CISSP
- CISM
- CEH
- CompTIA Security+
- ISO/IEC 27001 Lead Implementer / Lead Auditor
- CCSP
- GSEC
- Microsoft Security Certifications
- Cisco Security Certifications

Minimum Experience:

- Minimum seven (07) years in Information and Cyber Security.
- Minimum five (05) years of experience conducting cybersecurity awareness or professional training programmes.
- Demonstrated practical knowledge of current cybersecurity threats, attack techniques, cyber hygiene, and Government cybersecurity policies.
- Active contributor to cyber security domain on National and International level would be added advantage.
- Demonstrated experience implementing information security related Frameworks, Policies, Guidelines across multiple verticals would be added advantage.
- Be an active member of professional bodies in the domain of information and cyber security would be added advantage.

Additional Trainers

Where multiple programmes are conducted simultaneously, the Service Provider shall ensure the availability of an adequate number of qualified trainers with similar qualifications and experience.

All trainers shall be subject to the approval of Sri Lanka CERT.

Sri Lanka CERT reserves the right to reject any proposed trainer who does not meet the required competency level.

7. Review and Acceptance Procedure

Sri Lanka CERT shall appoint a Review Committee or Technical Evaluation Team to monitor the implementation of the assignment.

The Committee shall:

- Review all deliverables.
- Evaluate training materials.
- Observe selected training programmes.

- Verify participant records.
- Review evaluation results.
- Verify programme quality.
- Recommend acceptance of deliverables.

Where necessary, Sri Lanka CERT may request revisions or additional work before accepting any deliverable. Any revised deliverable shall be submitted within the timeframe specified by Sri Lanka CERT at no additional cost.