Terms of Reference (TOR): **Development and Revamp of the Disaster Management Center (DMC) Website**

1. Introduction and Background

The **Disaster Management Centre (DMC)** of Sri Lanka serves as the national focal point for disaster risk reduction, preparedness, emergency response, and recovery coordination. As part of its mandate, the DMC plays a critical role in ensuring timely dissemination of information, public awareness, and inter-agency collaboration during emergencies.

The existing DMC public-facing website (**www.dmc.gov.lk**) was developed several years ago and no longer meets modern standards for accessibility, security, user experience, or real-time performance. Its current limitations hinder the Centre's ability to communicate critical information quickly and effectively to citizens, stakeholders, and partner agencies.

To address these gaps, the DMC intends to undertake a **comprehensive revamp and modernization** of its official website. The new digital platform will serve as the **secure, resilient, and high-performing national hub** for crisis communication, early warnings, and coordination tools, supporting both day-to-day operations and rapid information dissemination during emergencies.

2. Objectives of the Assignment

The primary objectives of this assignment are to:

- Execute a complete revamp of the official Disaster Management website to align with updated web standards, best practices, and enhanced functionality.
- Establish the website as a reliable, real-time communication tool, critical for public safety during disaster preparedness and response.
- Achieve full compliance with all mandatory national security (Sri Lanka CERT) and accessibility (WCAG 2.1 Level AA) guidelines.
- Integrate securely with existing DMC and government backend systems (DIMS/ERP/ARP) and external Geographic Information Systems (GIS).

3. Scope of Work

The selected vendor will be responsible for the full lifecycle delivery, from architecture design through deployment, security clearance, and post-launch maintenance.

3.1 Core Operational and Functional Requirements

The platform must support the following essential capabilities:

- **Website Revamp:** Design and develop a responsive, modern interface following government digital branding guidelines, replacing the current outdated platform.
- **Content Management System (CMS):** Implement a robust, user-friendly CMS utilizing the **latest and stable version** of the chosen platform. Preference will be given to solutions that are open-source, widely supported, and compliant with government security and hosting standards.
- **Real-Time Alert Module:** Implement a mandatory functional module capable of broadcasting real-time incident notifications, advisories, and status updates, consistent with modern emergency management standards.
- **Data Visualization & Resource Mapping:** Support the display of location-specific disaster information, requiring the capability for seamless integration with external Geographic Information Systems (GIS) and spatial data layers.
- **General Features:** Document repository, multimedia gallery, and secure feedback/contact modules for incident reporting.

3.2 Mandatory Multilingual and Accessibility Standards

The website must be fully accessible and multilingual to serve the entire population:

- **Accessibility Threshold:** The vendor **SHALL** ensure full conformance to **WCAG 2.1, Level AA** as a mandatory technical threshold for all content and interfaces.
- **Multilingual Support:** The website **MUST** support **Sinhala, Tamil, and English**.
- **Multilingual Architecture:** The vendor **MUST** implement Multilingual Search Engine Optimization (SEO) best practices, including the **hreflang attribute** and an optimized **subfolder URL structure** (e.g., /si/, /ta/).
- **User Experience (UX):** The language switching mechanism **MUST** be highly visible (e.g., in the header) and **display the language name in its native script** (e.g., "සිංහල") for easy recognition. The user experience and functionality **MUST** be comparable across all language sites.

3.3 Strict Security and Compliance Mandates

Compliance with national government security standards is non-negotiable. The vendor must adhere to all guidelines issued by the Information and Communication Technology Agency (ICTA) and Sri Lanka CERT:

- **Domain and Hosting:** Mandatory use of the**.gov.lk domain name** and hosting provisioned in strict accordance with CERT Technical Guidelines.
- **Hosting Management Responsibility:** It is acknowledged that the hosting infrastructure (e.g., Lanka Government Cloud) is provided and managed by the DMC/Government of Sri Lanka. The vendor's responsibility is limited to the successful **deployment, configuration, security hardening, and ongoing maintenance of the application and its dependencies** on the mandated government platform.
- **Security Development:** All design and development **SHALL** incorporate security risks published in the **OWASP Top 10** as mandatory mitigation considerations.
- **Input Validation:** Robust input validation **SHALL** be implemented on both the client and server sides. Malware detection through scanning **IS ESSENTIAL** for all uploaded attachments.
- **Backend Access: Multi-factor Authentication (MFA)** and **Two-way SSL authentication MUST** be established for all users accessing the CMS or backend systems.
- **Encryption:** Sensitive information **MUST** be encrypted in transit (HTTPS/SSL for all public access) and at rest (in databases and backups).
- **Mandatory Security Assessment:** A comprehensive security assessment (VAPT- Vulnerability Assessment and Penetration Test) **MUST** be carried out by **Sri Lanka CERT prior to the production release**. The vendor must accommodate the required time for the assessment and any subsequent remediation.

3.4 Quantified Non-Functional Requirements (QNFRs)

The system is classified as a **Tier-1: Mission-Critical System**. Performance and resilience must be contractually guaranteed:

Requirement Category	Metric	Mandatory Value
Availability (Uptime SLA)	Annual Uptime Guarantee	99.9%
Resilience (RTO)	Recovery Time Objective (Max restoration time)	≤ 30 Minutes
Data Integrity (RPO)	Recovery Point Objective (Max acceptable data loss)	≤ 5 Minutes
Performance	Page Load Speed (First Contentful Paint)	≤ 3 Seconds (90th percentile)
Scalability	Peak Load Capacity (Concurrent Users)	Quantified Proposal (Min: 50,000 CU)

Note on Infrastructure and QNFRs: These QNFRs represent **mandatory performance outcomes** for the final deployed system. The vendor's technical proposal (Section 8.1) **MUST** detail the specific architectural components (e.g., load balancing, content delivery network (CDN) strategy, database replication) required to guarantee these metrics when hosted on the specified government infrastructure (e.g., Lanka Government Cloud or mandated data center.

3.5 Mandatory System Integration and API Strategy

The vendor **MUST** adopt an **API-first design strategy** and implement secure interoperability with existing government systems:

- **API-First Rationale:** The adherence to an API-first methodology is crucial because it ensures interfaces (APIs) are designed first—before any code is written—to act as the standardized and secure data exchange layer between the new website (front-end) and external core systems (DIMS/ERP). This decoupling enables secure access, reliable versioning, and allows the core systems to be updated independently of the public website.
- **Mandatory APIs:** The vendor **MUST** develop secure, versioned, RESTful APIs for predefined endpoints necessary to connect with the Disaster Information Management System (DIMS), Resource Databases, or ERP/ARP systems.
- **API Security:** API cybersecurity **SHALL** be designed following **Zero Trust principles** and secure coding practices, utilizing robust **Authentication and Authorization (A&A) mechanisms** (e.g., OAuth 2.0).
- **Testing:** Automated testing procedures **MUST** be established within the Continuous Integration/Continuous Delivery (CI/CD) pipeline to detect integration errors from external system changes.

4. Deliverables

The selected vendor shall submit the following deliverables, with the schedule incorporating the mandatory external security compliance phase.

Deliverable Name	**Estimated Duration**	**Brief Description**	**Key Expected Outcome/Strategic Value**
Inception Report	2 Weeks	Detailed work plan, methodology, final project timeline, and Project Governance Framework.	Establishes project foundation, aligns expectations, and defines governance.
Wireframes / Prototype	1 Week	Design mock-ups, architecture, and preliminary API specifications.	Provides the design foundation and initial user experience validation.
Beta Website (Internal QA)	8 Weeks	Functional demo with all modules, comprehensive API development, and	The system is complete with all functions and ready for rigorous external

		internal security testing.	audit.
Mandatory Security Clearance Phase	1 Weeks	Vendor facilitates and accommodates a full **Security Assessment by Sri Lanka CERT**. Includes time for vendor remediation of identified vulnerabilities.	**Mandatory Minimum Quality Threshold** clearance for production release.
Final Website & Deployment	1 Week	Fully tested, secure, and hosted platform, successfully cleared by Sri Lanka CERT and meeting all QNFRs (RTO/RPO).	Production-ready, resilient, and compliant platform launch.
Training & Documentation	1 Week	Comprehensive documentation (User Manual, Technical Documentation, Backup Procedures) and staff training.	Ensures sustainable operation and knowledge transfer.
Maintenance Phase	12 Months (Post-launch)	Ongoing technical support, security patching, and updates (Mandatory SLA with defined response times).	Ensures long-term security patching and system updates.

5. Duration of the Assignment

The total duration for the development, testing, mandatory security clearance, and final deployment is expected to be approximately **14 weeks (3.5 months) or less**, followed by a mandatory **one-year maintenance period**.

6. Qualifications of the Firm / Vendor

To ensure the successful execution of this nationally significant website revamp initiative, the selected vendor should demonstrate a well-rounded combination of **technical competence, functional understanding, and effective project management capability**. The firm should have proven experience in delivering ICT or web-based solutions of similar scope and complexity, preferably for government or large institutional clients.

6.1 Essential Technical Expertise

- **General ICT and System Development:**
  The firm should have relevant experience (ideally 5–7 years) in the development and deployment of ICT or web-based systems. Experience with modern development practices, cloud or hybrid hosting environments, and maintaining scalable, reliable solutions will be considered an advantage.
- **Web Design and CMS Development:**
  Demonstrated experience in designing and developing responsive, multilingual websites with an intuitive user interface. The vendor may utilize commonly adopted open-source CMS platforms such as WordPress, Drupal, Joomla, or equivalent. Familiarity with accessibility and usability standards (e.g., WCAG 2.1 Level AA) is expected.
- **Security and Compliance:**
  Experience in implementing secure web solutions that follow recognized security best practices, including mitigation of vulnerabilities listed in the OWASP Top 10. Vendors should be familiar with Sri Lanka CERT and ICTA guidelines for public sector systems and capable of applying appropriate security configurations such as SSL/TLS encryption and secure authentication mechanisms.
- **Data and System Integration:**
  Capability to integrate external data sources and APIs, including GIS layers or visualization tools, as part of a public-facing platform. Experience in connecting websites to secure backend systems or databases in a reliable and efficient manner will be an advantage.
- **Performance and Reliability:**
  Proven ability to design and deploy optimized, high-performing websites capable of handling high user traffic. Familiarity with hosting optimization, caching, data backup, and recovery mechanisms to ensure business continuity is desirable.
- **References:**
  The firm should provide at least two (2) references from similar projects completed within the past five (5) years. Each reference should include the project name, client organization, brief scope of work, and contact details for verification.

6.2 Essential Functional and Project Management Expertise

- **Public Sector or Institutional Experience:**
  Prior experience working with government, semi-government, or large institutional clients will be considered an advantage, particularly where adherence to public sector standards and reporting requirements was required.
- **Requirements and User Experience (UX):**
  Proficiency in gathering and documenting both functional and non-functional requirements and translating them into practical, user-friendly designs. The vendor should demonstrate experience in creating accessible and multilingual user experiences.
- **Project Management and Risk Handling:**
  Demonstrated ability to manage ICT projects effectively from initiation to completion within defined timelines and budgets. Experience applying structured project management methodologies, risk mitigation practices, and progress reporting mechanisms is expected.
- **Training and Change Management:**
  Experience in conducting capacity-building and knowledge transfer activities for client staff, including user training, content management handover, and post-deployment support to ensure sustainable system adoption.

7. Reporting and Coordination

The vendor will report directly to the Project Steering Committee and will work in close coordination with the DMC - ICT Units. Regular progress meetings and reviews will be held **biweekly** or as agreed upon.

8. Evaluation Criteria

The evaluation will employ a **Quality and Cost Based Selection (QCBS)** method, prioritizing technical quality and compliance with a **80% Technical / 20% Financial** weighting ratio.

Evaluation Category	**Sub-Criterion**	**Proposed Weighting (%)**	**Description**
I. Technical Proposal & Expertise	**80%**		
I.A. Technical Approach & Methodology (QNFRs)	30%	Soundness of architecture, API strategy, and **realism of the methodology** for delivering RTO/RPO (mins) and Peak Load	

		capacity (50,000 CU).	
I.B. Experience in similar projects and organizational Capacity	20%	Relevance of past projects; and organizational capacity/stability (assessed via financials).	
I.C. Team Composition & Expertise	15%	Qualifications and experience of key personnel (Lead, Security Engineer, Architect);	
I.D. Security & Mandatory Compliance (MQT)	15%	Detailed plan to meet **all Sri Lanka CERT mandates** (MFA, Two-Way SSL, OWASP mitigation, PEN Testing accommodation) and **WCAG 2.1 Level AA** compliance.	
II. Financial Cost (Price)	**20%**	Reasonableness and competitiveness of the budget; clarity of cost breakdown for development, and the mandatory 12-month maintenance period.	
Total	**100%**		

09. Ownership and Confidentiality

All data, source codes, and digital assets developed under this project shall remain the property of the Disaster Management Center (DMC). The vendor must ensure confidentiality and non-disclosure of any information accessed during the assignment.

Submission Requirements

Interested firms are requested to submit the following mandatory documents:

Technical Proposal (Mandatory)

- A cover letter expressing interest.
- Detailed methodology and work plan addressing all functional, security, and integration requirements.
- Detailed plan for meeting the stringent QNFRs (RTO, RPO, Peak Load).
- Curriculum Vitae (CVs) of key personnel, highlighting relevant experience and security certifications.
- List of at least two (2) similar projects successfully completed in the last five (5) years, including client references.

Financial Proposal (Mandatory)

- A detailed breakdown of all costs associated with the assignment, including professional fees, hosting recommendations, and the full 12-month maintenance cost.

Legal and Financial Documents (Mandatory Due Diligence)

- Copy of company registration certificate and Tax registration certificates.
- **Audited financial statements for the past three (3) years** to demonstrate financial stability and capacity.

Submissions (Mandatory Format)

- All submissions must be made in Hard Copy.