بسم الله الرحمن الرحيم

**Ministry of Homeland Security and Technology**
Republic of Maldives

**DIGITAL MALDIVES FOR ADAPTATION, DECENTRALIZATION AND DIVERSIFICATION (D'MADD) PROJECT**
**P177040**

# TERMS OF REFERENCE

**for**

## Hiring a Firm for TA to develop a business continuity and disaster recovery plan for the National Data Centre and National Computer Network

**Reference No: MV-MOECCT-DMADD-459312-CS-QCBS**

**Issued on:**
14/11/2024

**Advertisement no: (IUL)10-DMADD/10/2024/114**

## 1. INTRODUCTION

The Digital Maldives for Adaptation, Decentralization and Diversification (D'MADD) Project (P177040), aims to support the Maldives in its digital transformation. The D'MADD project is funded by a grant from the World Bank and is implemented by the Ministry of Homeland Security and Technology (MoHST). The key stakeholders include the National Centre for Information Technology (NCIT), the Communications Authority of Maldives (CAM) and the Department of National Registration (DNR).

The Project aims to enhance the enabling environment for the digital economy in Maldives, to improve identification for in-person and remote service delivery, and to leverage data and analytics for a green, resilient, and inclusive development. It is designed around three components, and the proposed activities are conceived following the country's priorities and funding needs in the medium term. The components are as follows:

**Component 1**: Enabling environment for improved digital connectivity and competitiveness

1.1. Improving regulatory frameworks, oversight, and enforcement for a competitive broadband market

1.2. Empowering public institutions for digital transformation in Government

**Component 2**: Digital identification for improved online and in-person service delivery

2.1. Legal and institutional enablers and safeguards for secure data and identity management

2.2. Modernizing of the foundational ID system and credential

2.3. Strengthening the digital authentication ecosystem

**Component 3**: Digital technologies and data platform for climate resilience

3.1. Establishing a climate data platform

3.2. Leveraging digital technologies and tools for climate adaptation

## 2. BACKGROUND

The Maldives experiences a variety of natural hazards, including cyclones, floods, sea swells, tsunamis, and fire hazards. Local thunderstorms, even of minor intensity, can cause significant damage due to the country's weak infrastructure. The Hulhangu Moosun season, characterized by heavy rainfall, leads to frequent flooding, particularly in the southern and central atolls. Coastal flooding from distant swells has caused significant damage, notably in April 1987 and May-June 2014. The eastern atolls, due to their proximity to the Sumatra subduction zone, are at high risk of tsunamis. Urban areas, especially those in the southern and central atolls, are increasingly vulnerable to fire hazards, leading to loss of life, property, and critical services. The recent cyberattacks on government agencies further emphasize the need for robust business continuity and disaster recovery plan.

The National Centre for Information Technology (NCIT) plays a critical role in the technological advancement and digital infrastructure of our nation. Assigned with the mandate to oversee the development and maintenance of critical government IT systems, NCIT serves as the backbone of our digital ecosystem.

Investment in digital technologies and infrastructure is crucial for the Maldives' growth, overcoming limitations posed by its land mass and dispersed population. Accelerating digital transformation requires investments in infrastructure, data platforms, and human capital.

Considering increasing threats like natural disasters and cyberattacks, a robust Business Continuity and Disaster Recovery (BCDR) plan is essential to ensure operational resilience and to facilitate the continuation of its operations in the event of disruption of business activities.

This Terms of Reference (TOR) will support subcomponent 1.2 of the DMADD project, “Empowering public institutions for digital transformation in government”, focusing on developing a BCDR plan for strategic digital government data assets and services to minimize downtime and data loss due to adverse events.

## 3. OBJECTIVE

The objective of this assignment is to engage a qualified firm (Consultant) to develop a comprehensive Business Continuity and Disaster Recovery (BCDR) plan for the National Data Centre (NDC) and the National Computer Network (NCN) operated by the NCIT. The Consultant is expected to identify risks to operations of NDC and NCN, develop, purpose policies, frameworks, and programs to assist manage business disruptions and well as tier up the NCIT resilience. Expected outcome of enhancing NCIT NDC/NCN Capability and ability of tackling likelihood as well as consequences of disruptive events human-caused or natural disasters.

The BCDRP should outlines the procedures, protocols, and strategies essential for maintaining critical operations of the NDC and NCN during and after a disaster or significant disruption and to prevent damage to the NDC and NCN. This should be in alignment with relevant industry standards (ISO 22301, ISO/IEC 27031, ISO/IEC 22237), laws (Disster Management Act) regulations, and best practices.

## 4. SCOPE OF WORK

The following scope of work outlines in general, the activities and responsibilities expected from the firm to successfully achieve the stated deliverables in section 5.

4.1. The consultant is expected to approach the BCDR plan with the utmost professionalism and expertise. The consultant should ensure that these plans are meticulously aligned with industry standards such as ISO 22301, ISO/IEC 27031, ISO/IEC 22237and regulatory frameworks, guaranteeing full compliance. Moreover, the consultant is to draw upon established best practices, leveraging proven strategies and methodologies to craft plans that not only meet local legal requirements but also embody the highest standards of operational excellence and resilience.

4.2. Stakeholder Engagement: The consultant will actively involve the key stakeholders, the National Disaster Management Authority (NDMA), the National Cyber Security Agency (NCSA), and the Communications Authority of Maldives (CAM), in the process. Their input is crucial to ensure the plans effectively align with national strategies and business objectives. This should involve facilitating workshops or meetings to discuss requirements, constraints, and expectations. The consultant will carry out pre-assessment discussions with the NCIT and work out a plan with clear coverage areas of analysis and content of the BCDR plan minimally described in Deliverable 1. The Consultant shall provide the guidance and shall include areas that the consultant deems necessary to be included in addition to the requirement

provided by the NCIT to ensure the BCDR plan adheres to industry standards and best practices.

4.3. Analysis of Current IT Infrastructure: The consultant must conduct a comprehensive evaluation of the existing NDC/ NCN infrastructure. This shall include but not limited to identifying all critical systems, components, and services that are essential for the day-to-day operations of the business. The analysis should cover the current business continuity and disaster recovery capabilities to understand the baseline from which improvements can be made.

4.4. Risk Analysis: Conduct a thorough risk analysis to identify potential threats to the business operations. This shall include but not limited to, staff competency, natural disasters, cyber-attacks, power failures, and any other relevant threats including availability of funding and support process such as procurement. The consultant shall determine the likelihood of these events occurring and their potential impact on the business using a framework on risk evaluation (e.g. tools recommended by Global Facility for Disaster Reduction and Recovery (GFDRR), with the aim of developing a prioritized list of risks to address in the continuity plan.

4.5. Business Impact Analysis (BIA): The NDC hosts mission critical systems of other government entities. The Consultant must keep this in consideration and analyse the potential effects of disruptions in the operation of NCIT /NDC and NCN. The BIA shall prioritize systems and processes based on their criticality to the Government, determining which functions are vital for the operations of the NCIT and other government agencies supported by the NCIT and the maximum tolerable downtime for each.

4.6. Strategy Development: The consultant, based on the findings from the risk analysis and BIA, must develop strategies for maintaining operations during and after a disaster. This will include proposing solutions for data backup, system redundancy, and failover procedures to ensure that critical functions can continue or be quickly restored. Additionally, it should consider specific resiliency/adaptation measures to better protect infrastructure assets against different types of natural hazards and other potential hazards (e.g. fire, break-up, etc.)

4.7. Compilation of the BCDR Plan (First Draft): The consultant shall draft a BDDR plan that includes detailed response and recovery procedures, clearly defined roles, and responsibilities. The plan will be designed to be actionable and straightforward to implement in the event of a disaster.

4.8. Implementation Guidance: Recommendations for the implementation of the BCP and DRP will be provided, including the necessary steps to take to put the plans into action. The consultant will also suggest training programs and exercises to prepare staff for potential disruptions, ensuring they are well-equipped to respond effectively.

4.9. Testing and Maintenance: The consultant will outline a schedule for regular testing and updating of the BCP and DRP to ensure they remain effective over time. This includes adapting the plans to reflect any changes in the business environment or infrastructure, as well as lessons learned from tests and actual events.

4.10. Documentation and Reporting: All findings, recommendations, and plans must be thoroughly documented. This should include range of items such as templates specific forms or checklists to be used by the NCIT. The consultant will prepare reports for management review and approval, ensuring transparency and accountability in the planning process.

**The consultant is expected to have at least two in-person missions during the consultancy in the Male' City**.

## 5. DELIVERABLES AND TIMELINE

Based on the above-described general scope of work for this assignment, in close coordination with PMU and DNR, Consultant shall be responsible for delivering the below outputs:

| Deliverables | Duration (Calendar Days) |
|---|---|
| **Deliverable 1:** The BCDR Plan Outline: It should include an approved list of coverage areas, ensuring that all critical aspects are addressed. This outline should be finalized after the stakeholder engagement workshop (in-person).<br><br>Business Continuity Plan<br>• Business Continuity Policy<br>• Business Impact Analysis (BIA) Report<br>• Risk Analysis Report<br>• Business Continuity Strategy Document<br>• Incident Response Plan<br>• Emergency Contact List<br>• Communication Plan<br>• Training and Awareness Materials<br>• BCP Test and Exercise Reports<br>• BCP Maintenance and Review Schedule<br>Disaster Recovery Plan<br>• Disaster Recovery Policy<br>• IT Infrastructure Analysis<br>• Critical Applications List<br>• Data Backup Procedures<br>• Recovery Procedures<br>• Site Recovery Plan<br>• DRP Test and Exercise Reports<br>• DRP Maintenance and Review Schedule | 15 |
| **Deliverable 2:** Comprehensive Analysis Report<br><br>This deliverable will combine the IT Infrastructure Analysis Report and the Risk Analysis Report into one comprehensive report. It will detail the current state of the NDC and NCN, identify critical systems, and evaluate potential risks and their impact on the business. The report will also include the Business Impact Analysis, prioritizing systems based on criticality and determining maximum tolerable downtimes. | 30 |

| | |
|---|---|
| **Deliverable 3:** First Draft of BCDR plan along with Strategic Continuity and Recovery Strategies<br><br>The third deliverable will be the first draft of BCDR plan which includes strategies that outlines the business continuity and disaster recovery strategies. It will propose actionable plans for data backup, system redundancy, and failover procedures, response plan and recovery procedures ensuring that operations can be maintained or quickly restored after a disruption. | 30 |
| **Deliverable 4:** Implementation and Training Guide<br><br>This guide will serve as a step-by-step manual for implementing the strategies outlined in the BCDR plan. It must include recommendations for staff training programs and preparedness exercises, ensuring that all personnel are equipped to respond effectively in the event of a disaster.<br><br>Testing Protocol and Maintenance Schedule: A schedule for regular testing and updating of the BCDR Plan must be provided to ensure they remain effective and relevant. This deliverable will outline the frequency of tests, maintenance activities, and the process for updating the plans based on test results and changing business needs. | 15 |
| **Deliverable 5:** Final Documentation and Presentation of The BCDR Plan to the stakeholders (in-person)<br><br>The final deliverable will encompass all documentation, including the BCDR plan, compliance and best practices guide, and a summary of stakeholder engagement. It will also include management reports for review and approval, ensuring transparency and accountability. | 30 |
| ***Total Duration*** | 120 |

## 6. PAYMENT SCHEDULE

Payment will be made in proportion to the contract terms upon submission of each deliverable, conditional upon the DNR's approval of the said deliverable.

| Deliverables | % |
|---|---|
| Deliverable 1 and 2 | 40 |
| Deliverable 3 | 30 |
| Deliverable 4 and 5 | 30 |

The selected firm shall be entitled to an advance payment of 10% of the total contract amount. This payment will be made upon the signing of the contract and submission of an advance payment guarantee. The advance payment guarantee must be issued by a reputable bank and be acceptable to the World Bank. The advance payment must be claimed within 45 days from the date of contract signing. The advance payment will be deducted from subsequent payments as per the payment schedule outlined in this contract.

## 7. INTELLECTUAL PROPERTY

All information pertaining to this project (documentary, audio, digital, cyber, project documents, etc.) belonging to the client, which the Consultant may come into contact within the performance of his/her, duties under this consultancy shall remain the property of the client who shall have exclusive rights over their use. Except for purposes of this assignment, the information shall not be disclosed to the public nor used in whatever manner without written permission of the Client in line with the national and International Copyright Laws applicable. All the material used in the project should be provided to the client with copyrights cleared.

## 8. INSTITUTIONAL ARRANGEMENTS, REPORTING AND SUPERVISION

8.1. The consultant will work under the guidance and direction of the NCIT and the D'MADD PMU will be coordinating the assignment.

8.2. Unless approved and agreed by the D'MADD PMU, the consultant shall not directly communicate, obtain, or share any documentation with any other party except NCIT.

8.3. The consultant shall report to the Project Manager of the D'MADD Project PMU and NCIT, on the status of the assignment on a regular basis. The consultant will work in a place agreed with the PMU and will be required to take part in all the relevant meetings.

8.4. All reports shall be submitted as stipulated in the deliverables and all reports will be submitted as drafts and upon review by the NCIT, the Consultant shall revise the draft reports. Once the revised reports are accepted by NCIT they will be termed as final reports by the PMU to process the payments.

8.5. All draft documents should be in Microsoft Word and all final documents in Adobe Acrobat format with relevant signatures where needed.

8.6. The Consultant shall ensure that all outputs are delivered on time, and in accordance with quantity, quality and timeframe in the proposal submitted by the consultant based on the TOR.

## 9. QUALIFICATIONS AND EXPERIENCE

9.1. Requirement of the Firm

- Minimum three (3) years of proven experience in information and communication technology infrastructure planning and development projects or consultancy services related to similar assignments.
- Minimum one (1) successfully completed project in business continuity, disaster recovery, or a related field.

**Note:** The maximum number of firms to be shortlisted will be 8. If the total number of qualified firms exceeds 8, the ranking will be determined based on the number of completed projects in business continuity, disaster recovery, or a related field.

9.2. Requirement expertise of the team

The firm is expected to propose a team of two (2) members. All the requirements given below should be met by the team collectively (i.e. at least one team member should meet any of the requirements). The firm should assign a team leader who will oversee the project, coordinate team efforts, and ensure timely delivery of project milestones. To ensure that a portfolio of previous projects and work done by all team members should be submitted.

**Team Leader**

- Master's degree in Business, Information Technology or related field with three (3) or more years in business continuity/ disaster recovery, business planning or related field. Official transcripts are required.
- Proven three (3) years of experience in business continuity, disaster recovery, business planning or a related field.
- Business Continuity certification from Disaster Recovery Institute International, Business Continuity Institute, or ISO 22301, ISO/IEC 27031, ISO/IEC 22237 preferred.

**BCDR Specialist**

- Bachelor's degree in Business, Information Technology, or a related field. Official transcripts are required.
- Proven two (2) years of experience in business continuity, disaster recovery, or a related field.
- Familiarity with relevant regulations and standards (e.g., ISO 22301).
- Strong analytical, problem-solving and documentation skills.

## 10. REQUIRED DOCUMENTS

10.1. Reference letters and certifications as proof of the qualifications and experience in Section 9. The reference letters may include project/ work experience letters as well as contract services successfully provided as a consultant (firm).

10.2. Documentation evidence providing evidence of the use of specific tools. This may be highlighted in reference letters of certificates on training for the specific tool.

## 11. SUBMISSION

**Project Manager**
Digital Maldives for Adaptation, Decentralization and Diversification Project (D'MADD)
Ministry of Homeland Security and Technology
NCIT Building
No 64, Kalaafaanu Hingun, Male' 20064, Republic of Maldives
Tel: +(960)330-2253
Email: procurement.dmadd@mohst.gov.mv

## Document Checklist for Submission of Expression of Interest

*(to be filled out by the consultant)*

**Assignment Title:** Hiring a Firm for TA to develop a business continuity and disaster recovery plan for the National Data Centre and National Computer Network

**Reference No.:** MV-MOECCT-DMADD-459312-CS-QCBS

**Advertisement No.:** (IUL)10-DMADD/10/2024/114

| ✓ | Required Documents |
|---|---|
| ☐ | Letter of Expression of Interest (Consultants may associate with other firms to enhance their qualifications, but should indicate clearly whether the association is in the form of a joint venture) |
| ☐ | Organization's governing documents as proof of registration |
| ☐ | Oorganizational Profile |
| ☐ | Reference letters and certifications or document evidence as proof of the experience (Firm) |

**Declaration:**

I, the undersigned, declare that the information provided in this Expression of Interest is accurate and complete to the best of my knowledge. I understand that any false statements may result in disqualification from the procurement process.

**Filled by:**

**Name and Position:**

**Signature:**

**Date:**