NKANGALA DISTRICT MUNICIPALITY

PROJECT: 54364
DEVELOPMENT, MAINTENANCE AND MONITORING OF ICT ENTERPRISE BUSINESS CONTINUITY PLAN, MSP AND DISASTER RECOVERY FOR NKANGALA DISTRICT MUNICIPALITY FOR A PERIOD OF THREE (03) YEARS. (RE-ADVERT)

SCOPE OF WORK

1. BACKGROUND

The NDM is committed to the improvement of quality of life for all in that it recognises Business Continuity Management (BCM) as one of the cornerstones of sound and responsible municipal governance. Key among the responsibilities of the municipality is to ensure continuity of the services during business interruptions.

Nkangala District is embarking on a project to appoint a service provider for the ongoing development/ review, maintenance/ monitoring of the enterprise business continuity management and disaster recovery plan of the district.

Business Continuity Management (BCM) is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders and reputation.

Business Continuity Plan (BCP) is a document which guides an organization in recovery from a significant loss or event back to delivering the key business functions of the organization. This plan will be based on the Business Continuity Management Policy which also needs to be reviewed and developed by the service provider. Implementation of the Business Continuity Plan will keep the operations of the business going during the most challenging and unexpected circumstances, protecting staff, preserving the organizational reputation and providing the ability to continue to operate. Furthermore, the BCP will cover all offices of the organization.

One of the major risks identified and highlighted by the municipality is the inadequate management of the business continuity management in the district and its local municipalities. This risk may have a serious impact on the effective and efficient delivery of services offered by the municipalities.

2. PROBLEM STATEMENT

There are various risks, threats and vulnerabilities that exist in the world today to which the organization may be exposed. These risks include but are not limited to the following:

- natural disasters such as floods, earthquakes and fire.
- accidents.
- service delivery protest.
- sabotage.
- power disruptions.
- Points of failure (outages due to an application error, hardware or network failure).
- communications, transportation, safety and service sector failure.
- environmental disasters such as pollution and hazardous materials spills; or
- Cyber-attacks and hacker activity.
- Pandemic outbreaks (Communicable and non-communicable diseases).

Some of the risks indicated above come unwarned and most of them never happen. The key is to be prepared and be able to respond to the event when it does happen, so that the organization survives; its losses are minimized; it remains viable, and it can be “business as usual”.

Therefore, by creating and maintaining a BCP and disaster recovery Plan (DRP) we will help ensure that the district municipality and its local municipalities have the resources and information that will be needed to deal with these emergencies.

3. THE OBJECTIVES OF THE PROJECT

To develop Business Continuity Plans and Disaster Recovery Plans for the district and local municipalities which must at least consist of:

- Identifying mission critical activities within critical processes in the organization’s functions and operations;
- Determining the impact of losses of each critical activity and the underlying technology dependencies of each activity;
- Identifying risks pertaining to the critical activities, operations and services;
- Providing a plan to maintain or restore critical operations during an unexpected event and communicate with key people so that they know their roles and responsibilities in the event of an unexpected incident and respond following a recognised practiced and agreed procedures. This will ensure that the most important functions, services and systems that are critical to the running of the department are up and running within the shortest possible time frame;
- Test the effectiveness of the Plans
- Enabling critical services to be continually delivered as per agreed service level agreements.
- Providing Business Continuity Plan implementation training to relevant staff and developing awareness programs; and

- Transferring skills to the Risk Management and information communication and technology team to enable ongoing review, maintenance and monitoring of the BCP and DRP.

4. SCOPE OF WORK

The scope of work to be conducted is for the district and its local municipalities **(**including their Directorates and sub directorates) and the organization's buildings.

4.1 Environmental analysis

Conduct environmental analysis through recognisable tools such as, amongst others, the SWOT/PESTEL, inclusive of a mitigating plan on threats and how NDM and local municipalities can leverage on opportunities.

4.2 Analysis Report

Provide analysis report on the existing policies, procedures and Standard Operating Procedures (SOPs).

4.3 Risk assessment, analysis and review

Complete/review risk analysis for critical functions and associated processes to identify likely risk events and their impact on operations.

4.4 Conduct Business Impact Analysis

a) Carry out Business Impact Analysis for all areas of operation according to a documented method. The BIA will quantify and record all skills, resources, services, infrastructure, interdependencies and supplies (both internal and external) required by each critical activity to achieve Recovery Time Objectives (RTO).
b) The BIA will prioritise restoration of activities and take into account tangible financial impacts of a disruption (increased cost of working, loss of revenue, fines, and penalties) and intangible and nonfinancial impacts (reputational, legal, regulatory, and customer servicing impact).
c) The BIA will reflect information on but not limited to:
   - Identified and defined critical service processes and/or functions
   - Critical success factors, peak periods (e.g. seasonal) and disruption threats
   - Maximum Acceptable outages (MAO)
   - Recovery Time Objective (RTO)
   - Recovery Point Objectives (RPO)

d) Identified recovery requirements will include but not limited to:
   - Information Technology dependencies and requirements
   - All information, procedures and processes required for the continuity of all critical activities including the recovery levels that must be achieved over time
   - An up to date inventory of the resources required over time to deliver the recovery strategies
   - Clearly identified locations at which recovery can take place
   - Continuity and resilience plan activation, roles, responsibilities and succession plans for unavailable staff.

4.5 Develop Business Continuity Strategy and Plan

a) Business Recovery Strategy will be developed to ensure that NDM and local municipalities can survive and remain resilient in disruptions and that their ability to drive continuity of their business is not compromised.
b) The Business Recovery Strategy will address the following but not limited areas:

- Resumption and recovery of the essential functions and services, their dependencies and supporting resources
- Mitigating, responding to and managing impacts
- Ensure the timely restoration of all affected critical activities and resources are fully up to date and reflect current service requirements, Business Impact Assessment (BIA) timeframes and priorities.

c) The continuity strategy processes will include but not limited to:
Identifying and documenting resource requirements based on BIA: The resources identified shall include but not be limited to;
- Information and data
- Facilities/Infrastructure
- Information Technology
- Operations and Production
- Finance
- People and Process
- External partners

d) Conducting gap analyses to identify gaps between recovery requirements and current capabilities Exploring recovery strategy options, based on the responses to the BIA questionnaire and taking into account the monetary and non-monetary impacts and assessing which divisions or functions should be prioritised.

e) The following should be addressed in the design, development and implementation of the Business Continuity Strategy;
- Incident Management Procedures
- Communication
- Operations Management
- Communication protocol
- Delegation of authority; and
- Recovery and restorations

f) The following are the minimum components the Business Continuity Plan shall contain;
- Purpose, scope and objectives of the plan
- Plan activation protocol and procedure
- Assumptions of the plan
- Essential services continuity priorities
- Implementation process
- Roles, responsibilities and authorities
- Communication requirements and procedures
- Internal and external dependencies and mode of engagement
- Continuity resource requirements
- Developing relocation plans
- Documenting manual workarounds
- Assembling the plans and having it validated by management

g) The Business Continuity Plan must fulfil the following attributes:
- Be securely stored in safe hard copy or electronic media;
- Be readily accessible by all of its authorized users;
- Contain related documents that are up to date and reflect the municipalities current requirements
- To support organizational continuity and resilience and dependant on the operational requirements, development and or review and maintenance amongst other of the following programs shall take place;
- Information Technology Disaster Recovery Plan
- Supply Chain Continuity; and
- Critical Infrastructure Program

- IT Disaster Recovery Plan (IT DRP)
- Crisis Management Plan (CMP)
- Emergency Response Plan (ERP)
- Provide advice on current alternative offsite (DR site) as well as data backup and offsite replication including servers, storage and network

4.6 Development of the Business Continuity Policy

Business Continuity Policy will be developed covering but not limited to the following areas:

- Identify the main threats in the organisation and possible threats to business processes
- Determine response tactics to losses that the business might incur due to a disaster
- Establish business unit plans that ensure continuity of business
- Drive all BCM activities to follow good practices in order to attain a full programme lifecycle
- Outline tools to be used throughout the BCM programme lifecycle; and
- Outline responsibilities of tactical committees and enhance BCM awareness

4.7 Measure Plan effectiveness through testing implementation

In order to validate and establish the reliability of the Business Continuity Strategy and Plan, the plans shall be tested. The test will further assist in establishing adequacy and confirm if plans meet the District and Local Municipalities' requirements.

a) The testing exercise shall be conducted in a manner that:

- Is consistent with the scope and the objectives of the BCM Policy, Strategy and Plan
- Is based on appropriate clearly defined aims and objectives
- Validate the continuity capability of NDM and Locals
- Minimise the risk of disruption of operations and maximise resilience
- Produce an actionable report containing the outcomes, recommendations and remedial action,
- Promote continual improvement

4.8 Review of the IT Master Systems Plan:

a) Review municipal documents to ensure the alignment of the IDP strategies to ICT trends
b) Design a future ICT Enterprise architecture/ IT Master Plan for the District by analysing the following:
   - Business architecture
   - Information architecture
   - Applications architecture
   - Technology architecture.
c) Develop IT Master Systems Plan that incorporates a 5-year Implementation Plan.

4.9 Develop a Disaster Recovery Plan

a) Develop/Review disaster recovery plan, operationalise and update to talk to the IT setup.
b) Prepare/review procedure manuals and team notes for disaster recovery.
c) Identify key documents and equipment for recovery plans and move copies to the recovery site.
d) Review IT Risk Register.
e) Develop IT Risk Management Procedures.
f) Review Change Control Procedure.
g) Develop/Review all IT Policies and Procedures in alignment with the Enterprise/ ICT BCP, DRP and IT Strategy.

4.10 Information Security Assessment:

a) Carry out IT security awareness initiatives and campaigns.
b) Oversee the monitoring of various Security control measures.
c) Proactively assess potential items of risk and opportunities of vulnerability in the network.
d) Design and monitor the implementation of IT Security policies and procedures on the network infrastructure, and workstations.
e) Carry out checks/ tests for effectiveness of Security controls on the network infrastructure.
f) Perform additional related responsibilities as required to ensure compliance with the Auditor General's requirements and relevant laws and regulations.

4.11 POPI and PAIA Assessment:

a) Conduct POPI and PAIA Readiness Assessment.
b) Develop a Plan of Action for POPI and PAIA Compliance that includes the development of a Data Protection Policy ‘and Procedures, and a Data Privacy Plan.
c) Conduct a Compliance Assessment to comprehensively evaluate how a Plan of Action is implemented to comply with POPI and PAIA.

4.12 Skills transfer to GPW project team

Ensure transfer of skill throughout various BCP steps for purposes of program maintenance and sustainability

5. OUTCOMES AND DELIVERABLES

5.1 The following deliverables are expected as the outcome of each phase during the project:

5.1.1 Business Continuity Management Framework
5.1.2 Business Continuity Management Policy
5.1.3 Business Impact Analysis report and Risk Assessment Report
5.1.4 Alignment to ICT Continuity Plans
5.1.5 Business Response Strategy
5.1.6 Business Continuity Management Response (Business Continuity Plan at District and Local Municipalities levels)
5.1.7 Testing of the BCP and DRP
5.1.8 Business Continuity and Disaster Recovery Training

6. Mandatory Technical Requirements

Bidders should take note of the following technical (quality) evaluation criteria.
All the necessary documentation must be submitted for the Evaluation Panel to make an informed evaluation. Evaluation of the Technical (Quality) Requirements will be based on the information provided by the bidder.

i. **Experience –** Bidders must only list projects of a similar nature undertaken in the past 5 years.
ii. **Expertise** – The qualifications of the resources that will undertake the work must be provided for evaluation purposes.
iii. **Methodology** – The bidder must clearly demonstrate how the contract will be managed, detailing a work plan with timeframes and clearly explaining how the different pieces of work will be implemented, in an integrated but seamlessly.

No	Business Process Area	Minimum required experience
1	Business Continuity & Disaster Recovery	Implementation of minimum 1 similar project in the Local Government sector
2	IT Disaster recovery	Implementation of minimum 1 similar project in the Local Government sector
3	IT Master Plan	Implementation of minimum 1 similar project in the Local Government sector
4	IT Governance	Implementation of minimum 1 similar project in the Local Government sector
5	Information Security	Implementation of at least 1 similar project
6	POPI or PAIA	Implementation of at least 1 similar project