

APPOINTMENT OF A SERVICE PROVIDER TO PROVIDE IT DISASTER RECOVERY AS A SERVICE (DRaaS)

SCOPE OF WORK

1. INTRODUCTION

CEF SOC Ltd is a state-owned company involved in the search for appropriate energy solutions to meet the energy needs of South Africa and the sub-Saharan African region. It also manages the operation and development of the oil and gas assets of the South African government. The company falls under the auspices of the Department of Mineral Resources and Energy (DMRE). For more information on the company you can visit our current website: www.cefgroup.co.za

2. BACKGROUND

Over the years, CEF has made significant investments to put in place standard processes and infrastructure that will ensure efficiency in its operations.

This increased dependency on technology coupled with an expansion in the scope and volume of services, business processes, transactions and regulatory requirements has created an increased risk of disruption to normal services.

Unforeseen incidents ranging from natural disasters, hardware failure, and information security breaches can have an adverse impact on a business and prevent it from continuing normal services.

To this end, CEF has implemented Business Continuity Management that aligns with the globally recognized ISO 22301, Business Continuity Institute Good Practice Guidelines, ISO 31000 and King IV. The BCM process encompasses emergency response, crisis management, business recovery and disaster recovery.

One of the key pillars of the BCM is IT disaster recovery. In terms of the BCM, IT is expected to implement recovery strategies to ensure that IT services, systems, infrastructure, hardware and software are able to be recovered within the Organisation's recovery requirements, specifically Recovery Time Objective (RTO) and Recovery Point Objective (RPO). To this end, IT seeks to implement IT disaster recovery.

3. IT LANDSCAPE

CEF SOC IT infrastructure is on-premise and fully virtualised on VMware platform located on one site in Sandton, Johannesburg. The infrastructure consists of the following:

3.1 Primary site

3.1.1 Hardware

The system consists of the following components:

- 5 x Dell VxRail S570 Hyper Converged Infrastructure nodes;
- 110TB Total SAN capacity (with 60TB used);
- 125Ghz CPU capacity (with 57GHz used);
- 1TB RAM (with 805Gb used, plan in place to be upgraded to 1.5TB);
- SonicWall NS3600 Firewall;

3.1.2 Core IT Infrastructure applications

CEF SOC IT Infrastructure use the following applications:

- Microsoft Windows Server 2016 Active Directory;
- VMWare 7.0;
- A total of 80 Virtual Machines running various Operating Systems (Windows Server 2008, 2012, 2016, 2019, and Linux);
- DMZ with 3 web servers;
- Microsoft Exchange server 2016;
- Mimecast email security and cloud-based archiving;

3.1.3 Networking

CEF SOC IT Network Infrastructure has the following components:

- Multiple VLANS (Voice, Server, Guest wireless, Business wireless, Workstations, DMZ);
- MTN ISP connection;

3.1.4 Business Applications

- VoIP based on Skype for Business 2016;
- ERP based Sage 300;
- Board Pack solution;
- Sage 300 People payroll;
- SQL Server (2014, 2016, 2019);
- BPM;
- VRM;
- IDU;
- SharePoint 2016;
- K2 Workflows;
- Assetware;
- Upside;
- CLA;
- TeamMate;
- Tasman;
- Betaal;

3.2 Backups

CEF IT currently performs backup using Veeam:

- Incremental backups to disk are done daily;
- Full backups to disk are done once a week;
- Weekly tape archiving is done and sent offsite;
- Monthly tape archiving is done and sent to offsite;

4. THE SCOPE

4.1 FULL DR REPLICATION ON THE CLOUD / DISASTER RECOVERY AS A SERVICE

CEF seeks to appoint a service provider for three (3) years to provide recovery of its data center services in an efficient and economically advantageous way, with minimal data loss and a rapid recovery time, as stipulated with the service-level agreements (SLA) for recovery-point objective (RPO) and recovery-time objective (RTO) tailored to meet our specific requirements.

The Disaster Recovery as a service (DRaaS) should replicate infrastructure, applications and data to the cloud to serve as a secondary site and enable full environmental recovery in the event of a disaster.

The cloud secondary site must effectively become the new environment and allow CEF to continue with daily business processes while the primary system undergoes repair.

4.2 REQUIREMENTS

4.2.1 DRaaS Requirements

- Rapid, effective, and testable recovery of targeted systems, services, or data in a declared disaster or when the primary site goes offline
 - DR capabilities for on-premises systems, services, and data
 - Readily and repeatedly testable at minimal or no cost
 - Testable during regular business hours with minimal or no impact to production systems, services, or data
 - Recovery Point Objectives (RPO's) of 4 hours or less
 - Recovery Time Objectives (RTO's) of 4 hours or less
- Full replication in the Cloud and distribution of the traffic between the on-premise site and cloud environments to allow CEF to recover
- In the event of a disaster or an emergency that causes CEF's on-premise environment to go offline, the solution must route all CEF's traffic to the cloud setup and scale appropriately.
- The DR solution at a minimum must have:
 - The ability to automatically backup critical systems and data,
 - The ability to quickly recover from a disaster, with minimal user interaction,
 - Flexible recovery options, such as restoring a single application or the whole infrastructure,
- Heterogeneous application-aware replication (Windows/Linux/UNIX Guest VMs)
- Partial Failover/Failback scenarios are supported
- End-to-end AES 256-bit encryption with built-in compression
- Disaster Recovery self-service testing, on-demand
- DRaaS management model: This must be a fully managed service

where the winning bidder takes over all responsibility for the planning, testing and management of disaster recovery, however, with some flexibility to allow CEF's involvement throughout the process, as and when it deems it necessary.

- A DRaaS subscription model is desired
- Preserve current VLANs configuration for easier failover;
- Provide 2 disaster recovery tests per annum;
- Provide 10 guaranteed seats reservation at the DR location with resources such as desk, chair;
- Provide both guest and business wireless infrastructure configured to work with DR infrastructure;
- Provide pricing schedule according to RPO and RTO with proposed Service level agreement (SLA);
- The winning bidder will be responsible for replication schedule;
- The winning bidder will be responsible for managing the link between CEF's premises to the DR;
- The winning bidder must have a data centre located in South Africa;
- The winning bidder must have multiple data centres for redundancy and failover purposes;

4.2.2 Implementation Requirements

- Provide key personnel who will be responsible for the implementation of the project and determine the roles, responsibilities and the team structure of such personnel. All key personnel dedicated to the project shall be properly qualified, possess valid certifications issued by the relevant vendor (if any)
- Document IT Disaster Recovery Strategy
- Document IT Disaster Recovery Plan
- Document IT Disaster Recovery Procedures
- Test of IT Disaster Recovery and signoff

4.2.3 Information and data security requirements

- **Strong Encryption Provides the Necessary Protection**

The first line of defense for data is robust, 256-bit AES encryption. All data must be encrypted whether it is at rest or in transit between CEF and DR site.

- **Control of encryption keys**

CEF desires having exclusive control over its data. To this end, CEF will engage the winning bidder and agree an arrangement for the control of encryption keys.

4.2.4 Service level requirements

- Recovery Point Objectives (RPO's) of 4 hours
- Recovery Time Objectives (RTO's) of 4 hours
- Two disaster recovery tests per annum
- Annual review and sign-off of the IT Disaster Recovery Strategy
- Annual review and sign-off the IT Disaster Recovery Plan
- Annual review and sign-off IT Disaster Recovery Procedures
- Frequent reporting and management visibility through an online portal,
 - Daily, weekly and monthly reports to be provided regarding replication status;
 - Alerts on replication failures

4.2.5 Other requirements

Given the critical nature of the recovery of CEF's data should the need arise; there are a number of requirements that the winning bidder must provide for.

- Adequate bandwidth for the replication as well as access to the DR in the cloud,
- All-inclusive pricing,
- The DraaS solution must incorporate file size management to reduce storage needs
- Failover assistance in a moment's notice,
- CEF's active involvement in DR testing,

4.3 Compulsory requirements

- The winning bidder will be responsible for managing the link between CEF's premises to the DR;
- The winning bidder must have a data centre located in South Africa;
- The winning bidder must have multiple data centres for redundancy and failover purposes
- Certifications
 - ISO 9001:2008
 - ISO 14001:2004
 - ISO 27001:2013
 - ISO/IEC 20000-1:2011

5. DELIVERABLES

5.1 Implemented Cloud Disaster Recovery solution

5.2 IT DR Plan

5.3 IT DR Strategy

5.4 Disaster Recovery Test

5.5 Disaster Recovery Procedures

6. PRICING

- All-inclusive pricing
- Subscription model
- Show monthly and annual costs, inclusive of VAT