

1. EVALUATION CRITERIA

1.1 PHASE 1

Administrative Evaluation Criteria

Initial Screening Process: At this phase bidder's response are reviewed to check if bidders have responded according to CEF (SOC) Ltd RFP document.

1.2 PHASE 2 Mandatory evaluation

The bidder must indicate its compliance / non-compliance to the requirements and should substantiate its response in the space provided below. If more space is required to justify compliance, please ensure that the substantiation is clearly cross-referenced to the relevant requirement. The Mandatory Technical Requirements are as follows:

Mandatory requirements	Comply	Not comply
1.2.1 The winning bidder will be responsible for managing the link between CEF's premises to the DR;		

1.2.2 The winning bidder must have a data centre located in South Africa;		
Provide relevant proof such as service agreement with data centre owner, proof of address, etc.		

1.2.3 The winning bidder must have multiple data centres for redundancy and failover purposes.		
Provide relevant proof such as service agreement with data centre owner, proof of address, etc		

1.2.4 Certifications • ISO 27001:2013 • ISO/IEC 20000-1:2011		
Provide certificate as proof		

Note: Failure to comply with any of the Mandatory Requirements may lead to the bidder being disqualified, and not considered for further evaluation on Other Technical Requirements.

1.2 PHASE 3 Technical evaluation

Bidders will be evaluated according to the below technical evaluation criteria. Minimum Technical Threshold is **80%**. It must be noted that if the Bidder does not meet the **80%** minimum threshold, the bidder will be disqualified and not be evaluated further.

1.3.1 Experience of the Bidder			
The bidder must have experience in providing DR as a managed service (DRaaS) as specified in this RFP.			
The bidder must provide reference letters from clients to whom DRaaS as described in this RFP are/were provided. The reference letters must be on a client's letterhead, and include the name, address and contact details of the client.			
5 and more reference letters	5	Signed reference letters on client letter heads	15%
4 reference letters	4		
3 reference letters	3		
2 reference letter	2		
1 reference letter	1		
0 no reference letter submitted	0		

1.3.2 Requirements

The bidder's proposed solution must meet the business requirements as specified in the document.

The bidder must provide a detailed proposal of DRaaS and Disaster Recovery services offered to fulfil each element of the scope of work/ business requirements. The bidder must complete and return the Business Requirements table below.

Meets 100% and more of requirements	5	Provide comments in terms of extent to which you meet each of the business requirement in Annexure A	55%
Meets 90-99% of requirements	4		
Meets 80-89% of requirements	3		
Meets 70-79% of requirements	2		
Meets 60-69% of requirements	1		
Meets less than 60% of requirements	0		

1.3.3 Team experience

The bidder's key personnel of the proposed project team must have relevant qualification, skills and experience in both DRaaS / Disaster Recovery services.

10 years and more	5	The bidder must submit CVs of the key personnel; and the CVs must clearly highlight areas of experience/ competence relevant to the tasks and objectives of this project	15%
8-9 years of experience	4		
6-7 years of experience	3		
4-5 years of experience	2		
1-4 years of experience	1		
Less than 1 year experience	0		

1.3.4 Approach and methodology

The bidder must demonstrate thorough understanding of the objectives and deliverables of this request by providing a detailed implementation plan with the following:

- Implementation guideline,
- work breakdown structure,
- milestones and related duration; and
- service level agreement post implementation.

The proposal fully meets expectation	5	The bidder must demonstrate thorough understanding of the objectives and deliverables of this request by providing a detailed implementation plan	15%
The proposal fairly meets expectation	4		
The proposal partially meets expectation	3		
The proposal does not meet expectation	0		

BUSINESS REQUIREMENT TABLE

Business Requirements for a fully managed DaaS / disaster recover service

The bidder must indicate its compliance / non-compliance to the requirements and should substantiate its response in the space provided below. If more space is required to justify compliance, please ensure that the substantiation is clearly cross-referenced to the relevant requirement.

TECHNICAL SOLUTION REQUIREMENTS

REQ#	Technical Requirements	Comply or Not Comply	Provide details of how your solution satisfies CEF requirements
1.	Rapid, effective, and testable recovery of targeted systems, services, or data in a declared disaster or when the primary site goes offline		
2.	DR capabilities for on-premises systems, services, and data		
3.	Readily and repeatedly testable at minimal or no cost		
4.	Testable during regular business hours with minimal or no impact to production systems, services, or data		
5.	Recovery Point Objectives (RPO's) of 4 hours or less		
6.	Recovery Time Objectives (RTO's) of 4 hours or less		
7.	Full replication in the Cloud and distribution of the traffic between the on-premise site and cloud environments to allow CEF to recover		
8.	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.		
9.	The ability to automatically backup critical systems and data,		
10.	The ability to quickly recover from a disaster, with minimal user interaction,		
11.	Flexible recovery options, such as restoring a single application or the whole infrastructure,		
12.	Heterogeneous application-aware replication (Windows/Linux/UNIX Guest VMs)		
13.	Partial Failover/Failback scenarios are supported		
14.	End-to-end AES 256-bit encryption with built-in compression		
15.	Disaster Recovery self-service testing, on-demand		
16.	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.		
17.	A DRaaS subscription model is desired		

18.	Preserve current VLANs configuration for easier failover;		
19.	Provide 2 disaster recovery tests per annum;		
20.	Provide 10 guaranteed seats reservation at the DR location with resources such as desk, chair;		
21.	Provide both guest and business wireless infrastructure configured to work with DR infrastructure;		
22.	Provide pricing schedule according to RPO and RTO with proposed Service level agreement (SLA);		
23.	The winning bidder will be responsible for replication schedule;		
24.	The winning bidder will be responsible for managing the link between CEF's premises to the DR		
25.	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.		
26.	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.		
27.	Two disaster recovery tests per annum		
28.	Annual review and sign-off of the IT Disaster Recovery Strategy		
29.	Annual review and sign-off the IT Disaster Recovery Plan		

30.	Annual review and sign-off IT Disaster Recovery Procedures		
31.	Daily, weekly and monthly reports to be provided regarding replication status;		
32.	Alerts on replication failures		
33.	Adequate bandwidth for the replication as well as access to the DR in the cloud,		
34.	All-inclusive pricing,		
35.	The DraaS solution must incorporate file size management to reduce storage needs		
36.	Failover assistance in a moment's notice,		
37.	CEF's active involvement in DR testing,		