

THE NATIONAL CREDIT REGULATOR

OCTOBER 2026

**TERMS OF REFERENCE FOR THE APPOINTMENT TO SELECT
OF A QUALIFIED AND EXPERIENCED SERVICES PROVIDER
TO ESTABLISH A DISASTER RECOVERY (DR) AND BUSINESS
CONTINUITY (BS) SOLUTION FOR PERIOD OF THREE (3)
YEARS AT NATIONAL CREDIT REGULATOR**

RFP NUMBER: NCR1047.10.2026

DUE DATE: 20 NOVEMBER 2026 AT 11H00 SHARP CAT
**ADDRESS: 127-15TH ROAD RANDJES PARK MIDRAND (NCR
OFFICES)**
EMAIL YOUR RFP QUERIES TO: procurement@ncr.org.za

PART A- GENERAL TERMS OF CONDITIONS (SCM)

1. General Information for Bidders

The National Credit Regulator (NCR) was established in terms of section 12(1) of the National Credit Act, Act 34 of 2005 and came into being on 1 June 2006.

The NCR will determine which bidding organisation ("bid participant"), if any, is appointed in response to this request for submission of the appointment of a service provider for the acquisition / procurement of qualified / accredited service provider / supplier internet service provider (ISP) for the provision of the internet and related.

General Terms

This tender is issued in terms of the Public Finance Management Act 1 of 1999 (PFMA), the Preferential Procurement Policy Framework Act 5 of 2000 (PPPFA), the Preferential Procurement Regulations, 2001/2022 (PPR), Supply Chain Management Regulations issued by the National Treasury and BBBEE Act.

Parties that wish to submit proposals are required to indicate that they are willing to accept the General Conditions and Procedures of the NCR (Annexure B and B.1 that can be downloaded from NCR website -<https://www.ncr.org.za/index.php/procument/tender-standard-bidding-documents/general-terms-conditions>). **Please read this document carefully and confirm your agreement to the terms prior to submitting your proposal.**

2. The Proposal Format

- **Economy of proposal preparation**

The proposal should be prepared simply and economically, providing a straightforward and concise description of the bid participant's ability to meet the requirements of the proposal request.

Clear factual responses are required. The content of the proposals shall determine the merit of each participant, not brochures or other marketing material. To facilitate the review of proposals, participants are required to organise their responses according to the format presented below. Should a participant wish to provide additional information, that information should be referred to and provided in a file of annexure.

3. Validity of proposals

The proposals must include a statement as to the period for which the proposal remains valid. The proposal must be valid for at least ninety (90) days from the due date for the submission of all bids.

4. Number of proposals

Each bid participant must provide two (2) hard copies **(original & copy)** and one (1) memory stick of their entire proposal, including all the documentation referred to in Section 7 below, in the format specified in that section. All submitted proposals will become the property of the NCR and will not be returned. The proposal must be signed and dated in black ink by the bidder or authorized representative of the bidder and initialled on each page.

5. Submission of proposals

- 5.1. Proposals must reach the offices of the NCR before 11:00AM on 31 August 2026 and must be enclosed in a sealed envelope which must be clearly labelled/addressed on the outside.

a) RFP No: NCR1047.10.2026

b) TERMS OF REFERENCE FOR THE APPOINTMENT TO SELECT OF A QUALIFIED AND EXPERIENCED SERVICES PROVIDER TO ESTABLISH A DISASTER RECOVERY (DR) AND BUSINESS CONTINUITY (BS) SOLUTION FOR PERIOD OF THREE (3) YEARS AT NATIONAL CREDIT REGULATOR

c) CLOSING DATE: 20 NOVEMBER 2026 AT 11H00 AM,

- 5.2. Proposals are to be submitted in the marked tender box, in the reception area, National Credit Regulator, 127-15th Road, Randjiespark, Halfway House, Midrand. The tender box will only be available for the depositing of proposals between 08h00 and 16h30 on weekdays (excluding public holidays).
- 5.3. Please note that this RFP closes punctually at 11h00 on 20 NOVEMBER 2026 No late submissions will be considered under any circumstances.
- 5.4. **All** the documentation referred to in Section 7 below must be submitted. Failure to submit all the documentation referred to in this section may result in a submission being discarded, and not considered for evaluation.
- 5.5. If responses are not delivered as stipulated in this Section 5.1, such responses will be considered **“late”**, and will not be considered for evaluation.

- 5.6. The NCR shall not disclose any details pertaining to the responses received, to any other participant, as this is regarded as confidential information.
- 5.7. Envelopes must not contain documents relating to any RFP other than the one referred to in this RFP.
- 5.8. The responses to the RFP will be opened as soon as is practical after the expiry of the time advertised for receiving them.
- 5.9. Only the participants that are short-listed after the evaluation process will be informed of the results of the submission adjudication process.
- 5.10. After the evaluation process is completed, the Evaluation Committee may, prior to making a final selection, draw up a shortlist of participants and require them to make a detailed presentation to the Adjudication Committee. A minimum of 2 days' notice will be given to relevant participants in advance of the presentation date.

6. Timetable

Date & time	Activity
19/10/2026	Issue RFQ document
20/11/2026	Closing date
21/11/2026	Preliminary evaluation
21/11/2026	Evaluations by the Evaluation Committee
25/12/2026	Adjudication Committee meeting
01/12/2026	Appointment

The National Credit Regulator reserves the right to determine the structure of the process, the right to determine the number of short-listed participants, the right to withdraw from the proposal process, and the right to change this timetable at any time without notice.

7. Documentation to be submitted.

Document that must be Submitted	Guideline		Consequence of Non-submission
Invitation to Bid – SBD 1	Yes	Complete and sign the supplied pro forma document	Disqualification from process
Tax status SBD 1	Yes	Written confirmation that SARS may on an ongoing basis during the tenure of the contract disclose the bidder's tax compliance status. Proof of Registration on the Central Supplier Database Vendor number	Disqualification from process
Declaration of Interest – SBD 4	Yes	Complete and sign the supplied pro forma document	Disqualification from process
Preference Point Claim Form – SBD 6.1	Yes	Non-submission will lead to a zero (0) score on Specific goals	Zero points awarded for specific goals
Registration on Central Supplier Database (CSD)	Yes	The Service Provider must be registered as a service provider on the Central Supplier Database (CSD). If not registered, to complete the registration of company prior to submitting the proposal. Visit https://secure.csd.gov.za/ to obtain your vendor number starting with MAAA. Submit proof of registration.	Disqualification from process
Acceptance of the General Terms and Conditions	Yes	https://www.ncr.org.za/index.php/procedure/tender-standard-bidding-documents/general-terms-conditions	Disqualification from process bidders to confirm that they read

8. Evaluation Criteria

Proposals will be evaluated on the 80/20 preference points scoring system: that is, 80% of the points awarded will be based on price, as indicated in the table below; and 20% of the points awarded will be based on specific goals, allocated as indicated in the table below:

B-BBEE status level of contributor	Specific goals	Price
Total maximum points	20	80

The points system is outlined for the 80/20 to address the preferential procurement as followed:

8.1. SMME's which are owned by Black people.

SPECIFIC GOAL	ACHIEVEMENT LEVEL	TOTAL NUMBER OF
Persons historically disadvantaged on the basis of race	81%- 100% black ownership	7
	51% - 80% black ownership	5
	31% - 50% black ownership	3
	0 – 30% black ownership	1

8.2. SMME's which are owned by People with disability

SPECIFIC GOAL	OWNERSHIP LEVEL	POINTS
Persons historically disadvantaged on the basis of disability	50 %- 100% owned by persons living with disabilities	3
	30% - 49% owned by persons living with disabilities	2
	0 – 29% owned by persons living with disabilities	1

8.3. SMME's which are owned by Women.

SPECIFIC GOAL	ACHIEVEMENT LEVEL	POINTS
Persons historically disadvantaged on the basis of gender – Women	81% - 100% black owned by women	7
	51% - 80% black owned by women	5
	31% - 50% black owned by women	3
	0 – 30% black owned by women	1

8.4. SMME's which are Youth owned business.

SPECIFIC GOAL	OWNERSHIP LEVEL	POINTS
	50%- 100% owned by persons who are youth	3

Persons historically disadvantaged based on age	30% - 49% owned by persons who are youth	2
	0 – 29% owned by persons who are youth	1

9. Evidence for specific goals

PROOF OF EVIDENCE TO SCORE SPECIFIC GOALS POINTS			
EVIDENCE	YES	NO	ATTACH EVIDENCE (indicate a page)
Share certificate			
ID Copies stamped by the commissioner of oath			
Sworn affidavits			
BBBEE certificates			
Proof of disability			
CIPC Documents			

NB: Bidders will only score points based on the evidence submitted.

10. Reporting of fraud and corruption

The National Credit Regulator management is commitment to transparency, integrity, and accountability, as described in our Code of Conduct and business principles. Which led to the establishment of the Ethics Line. The Ethics Line seeks to provide an independent and comprehensive service through enhanced anonymity assurance and a wide range of communication channels. Bidders and members of the public are encouraged to use the following toll-free line to report any misconduct relating procurement activities amongst others.

Fraud / Anti-Corruption Hotline

**Report any incidents of wrongdoing
to the KPMG Ethics Line**

800 53 17 (Toll Free)

PART B: NEXT PAGE

PART B: TERMS OF REFERENCE FOR THE APPOINTMENT TO SELECT OF A QUALIFIED AND EXPERIENCED SERVICES PROVIDER TO ESTABLISH A DISASTER RECOVERY (DR) AND BUSINESS CONTINUITY (BS) SOLUTION FOR PERIOD OF THREE (3) YEARS AT NATIONAL CREDIT REGULATOR

A.1 BACKGROUND AND CONTEXT

The National Credit Regulator (NCR) is the regulatory authority established on 1 June 2006 in terms of the National Credit Act, 2005, with the mandate to promote and advance the social and economic welfare of South Africans; to promote a fair, transparent, competitive, sustainable, responsible, efficient, effective and accessible credit market and industry; and to protect consumers.

A.2 PURPOSE

The purpose of this project is to appoint a qualified, accredited and reputable service provider to provide the NCR with a fully managed backup, disaster recovery and business continuity solution, including support and maintenance services, for a period of three (3) years. Two options are proposed for consideration: Option A, Cloud-Based Backup and DR as a Service (BaaS / DRaaS); and Option B, DR private hosting with dedicated infrastructure. The scope covers the complete in-scope workload set described in Section A.4 below, including physical and virtual infrastructure, the Windows Server environment, Active Directory, DNS, DHCP, file services, database and line-of-business systems, and Microsoft 365 workloads.

A.3 OBJECTIVES

- Extend the NCR's existing internal immutable backup capability to a fully managed platform with off-site protection;
- Achieve RPO of one (1) hour or less and RTO of four (4) hours or less across all in-scope workloads;
- Deliver demonstrable business continuity, including tested failover and failback, quarterly DR drills, and ransomware resilience;
- Enforce data sovereignty: all NCR data must be stored and processed within South Africa in Tier 3 or Tier 4 data centres;
- Evidence compliance with POPIA, ISO 27001/27002:2022, ISO 22301:2019, ISO 27018:2019 and the NIST Cybersecurity Framework;
- Provide 24x7x365 support, proactive monitoring, and a dedicated Project Manager and Infrastructure Architect; and

- Transfer knowledge and certify a minimum of two (2) NCR engineers on the platform.

A.4 CURRENT STATUS OF THE NCR ICT ARCHITECTURE

- A.4.1 The NCR operates from its main office at 127 - 15th Road, Randjespark, Midrand. The current office lease is expected to end in August 2026, and there is a possibility of relocation to a new building at the end of the current lease.
- A.4.2 Following the ransomware incident and the subsequent recovery programme, the production environment was rebuilt onto six standalone Microsoft Hyper-V hosts, hosting approximately fifteen (15) production virtual machines. The hosts are not clustered: each operates independently, with no automatic failover between hosts. The NCR's production applications and infrastructure services are hosted on this virtualised platform, with the exception of the two (2) Domain Controllers and the NCR File Server, which are hosted on dedicated standalone (physical) servers outside the Hyper-V host environment. The environment is summarised by functional component below:

Component	Description
Hyper-V hosts	HOST 1 through HOST 6 (six standalone Hyper-V hosts), each independently providing virtualisation for NCR production workloads. The hosts are not clustered. The two (2) Domain Controllers and the NCR File Server are hosted on separate dedicated standalone (physical) servers outside the Hyper-V host environment.
Identity and core infrastructure services	Certificate Authority, Network Policy Server, Azure Active Sync and NCR-VPN. DNS and DHCP are hosted as server roles on the Domain Controllers.
Business applications	Sage 300 People (Application and Database servers), Microsoft Dynamics GP (Application and Database servers), IRAS, Microfile, YSoft SafeQ print management server.
Web and application services	Internet Information Services (IIS) hosted on virtualised application servers, supporting internal and externally facing NCR web applications and services.
Messaging and collaboration	Exchange server, supported by Microsoft 365 (E5) online services for 250 users, including Exchange Online, SharePoint Online, OneDrive and Microsoft Teams.
ICT management and operations	Windows Admin Centre, Operations Manager, Patch Manager, Service Desk Plus, Nessus Vulnerability Scanner, AD Manager Plus, KM Print Server.

Component	Description
Operating platform	Microsoft Windows Server (2019 and 2025) with Microsoft SQL Server databases; total protected data volume estimated at approximately 50TB to 100TB, to be confirmed during the discovery phase.

- A.4.3 The environment runs Microsoft Windows Server operating systems (2019 and 2025) with Microsoft SQL Server databases, and hosts the NCR's mission-critical applications and infrastructure services, including both Domain Controllers (Active Directory, DNS and DHCP), Exchange, Sage 300 People (application and database), Microsoft Dynamics GP (application and database), IRAS, Microfile, YSoft SafeQ, the NCR File Server, IIS-based application and web servers, certificate services, network policy services, and ICT management tooling.
- A.4.4 The NCR holds a Microsoft 365 (E5) licence agreement for 250 users and uses Entra ID (Azure Active Directory) and Microsoft online services, including Exchange Online, SharePoint Online, OneDrive and Microsoft Teams.
- A.4.5 Dedicated, logically isolated backup storage provisioned across the NCR's standalone Hyper-V hosts serves as the internal backup repository. Backups are immutable and are stored in two separate locations, providing protection against ransomware and accidental deletion. This internal capability must be preserved and integrated into the proposed solution.
- A.4.6 The total protected data volume, including files, folders and onsite application systems, is estimated at approximately 50TB to 100TB. The precise figure is to be confirmed by the successful bidder during the discovery phase.
- A.4.7 The NCR currently has an interim off-site Disaster Recovery contract in place until 31 October 2026. The objective of this project is to replace that contract with the enhanced services described in these Terms of Reference.
- A.4.8 Consolidated DR Workload and Infrastructure Inventory
- A.4.8.1 The complete inventory of servers, systems, applications, databases, virtual machines, infrastructure components and services covered by the proposed backup, disaster recovery and business continuity solution is consolidated in the table below, together with indicative vCPU, RAM and storage specifications to inform bidder costing. Bidders must confirm coverage of every item as part of their technical response. The vCPU figures require confirmation before use, as set out in the footnote to the table.

No.	Server / Workload Name	System / Application	Business Function	Environment	vCPU†	RAM (GB)	Storage (GB)
-----	------------------------	----------------------	-------------------	-------------	-------	----------	--------------

1	HOST 1	Hyper-V Hypervisor	Virtualisation platform	On-Premises, Physical	4110†	120	2,000
2	HOST 2	Hyper-V Hypervisor	Virtualisation platform	On-Premises, Physical	4110†	120	2,000
3	HOST 3	Hyper-V Hypervisor	Virtualisation platform	On-Premises, Physical	4110†	120	2,000
4	HOST 4	Hyper-V Hypervisor	Virtualisation platform	On-Premises, Physical	2637†	120	2,000
5	HOST 5	Hyper-V Hypervisor	Virtualisation platform	On-Premises, Physical	4208†	120	2,000
6	HOST 6	Hyper-V Hypervisor	Virtualisation platform	On-Premises, Physical	4208†	120	2,000
7	DC1 (Primary Domain Controller)	Active Directory, DNS, DHCP	Identity, name resolution, address mgmt	On-Premises, Physical, standalone	4208†	32	808
8	DC2 (Secondary Domain Controller)	Active Directory, DNS, DHCP	Identity, name resolution, address mgmt	On-Premises, Physical, standalone	4208†	32	250
9	NCR File Server	Windows File Services	Shared file and folder storage	On-Premises, Physical, standalone	4110†	100	3,000
10	Ops Manager	Microsoft System Center Operations Manager	ICT infrastructure monitoring	On-Premises, Virtual (VM)	4110†	24	2,000
11	Apps Server	General application hosting	Application hosting	On-Premises, Virtual (VM)	4110†	24	999
12	Service Desk	ManageEngine ServiceDesk Plus	IT service management / helpdesk	On-Premises, Virtual (VM)	4110†	24	500
13	Patch Manager	ManageEngine Patch Manager	Patch management	On-Premises, Virtual (VM)	4110†	24	2,000
14	Great Plains	Microsoft Dynamics GP (Application)	Finance / ERP application server	On-Premises, Virtual (VM)	4110†	32	500
15	Great Plains SQL	Microsoft Dynamics GP (Database)	Finance / ERP database	On-Premises, Virtual (VM)	4110†	24	200
16	Sage App	Sage 300 People (App and Database)	Human Resources / Payroll	On-Premises, Virtual (VM)	4110†	24	500

17	Microfile	Microfile	Document and records management	On-Premises, Virtual (VM)	4110†	24	2,000
18	IRAS	IRAS (Application and Database)	Registrant / credit provider registration	On-Premises, Virtual (VM)	4208†	16	373
19	Intranet	Internal web application (IIS)	Staff intranet	On-Premises, Virtual (VM)	4208†	20	500
20	AD Sync	Microsoft Entra Connect	Directory sync to Microsoft 365	On-Premises, Virtual (VM)	4208†	20	100
21	Trend Secure Gateway	Trend Micro Secure Gateway	Email / web security gateway	On-Premises, Virtual (VM)	4208†	20	100
22	Net Policy Server	Windows Network Policy Server (NPS)	Network access policy / RADIUS	On-Premises, Virtual (VM)	4208†	20	100
23	Exchange	Microsoft Exchange Server	On-premises messaging	On-Premises, Virtual (VM)	4208†	20	100
24	CA Server	Certificate Authority	PKI / certificate services	On-Premises, Virtual (VM)	4208†	20	100
25	Print management server*	YSoft SafeQ	Print management	On-Premises (to be confirmed)*	TBC*	TBC*	TBC*
26	Microsoft 365 tenant	SharePoint Online	Document collaboration and storage	Cloud, Microsoft 365	N/A	N/A	N/A
27	Microsoft 365 tenant	OneDrive	Personal / departmental file storage	Cloud, Microsoft 365	N/A	N/A	N/A
28	Microsoft 365 tenant	Exchange Online	Hybrid / cloud messaging	Cloud, Microsoft 365	N/A	N/A	N/A
29	Microsoft 365 tenant	Microsoft Teams	Collaboration and communications	Cloud, Microsoft 365	N/A	N/A	N/A
30	Microsoft 365 tenant	Microsoft Entra ID	Cloud identity and access management	Cloud, Microsoft 365	N/A	N/A	N/A

* The server hosting the YSoft SafeQ print management service could not be separately identified in the current inventory extract and should be confirmed against the ICT asset register before the Terms of Reference are finalised.

† vCPU figures are carried over as extracted from the source server inventory and could not be verified: several unrelated workloads share the same figure and the magnitude (in the thousands) is inconsistent with a typical per-VM virtual core count. These values may reflect CPU clock speed (MHz) or another field captured in error during the inventory extraction, rather than allocated vCPU counts. RAM and storage figures are as recorded in the source

inventory. ICT must confirm actual vCPU allocations directly from Hyper-V Manager / System Center before this table is issued to the market for costing purposes.

A.5 EXPECTED OUTPUTS

- Configuration and takeover of the backup and DR services from the current service provider, with documented chain of custody;
- Internet line / connectivity between the NCR data centre and the DR site;
- Managed online / cloud backup facility, integrated with the NCR's internal immutable backup repository;
- Regular data backups and retention in accordance with NCR policies;
- Fully managed disaster recovery and restoration facilities in accordance with NCR policies (per folder, file, application system, and virtual machine);
- Fully managed virtual disaster recovery / secondary site;
- Three-year support and maintenance in line with NCR SLA requirements; and
- Structured handover of the services upon expiry of the contract, including data retrieval and certified sanitisation.

A.6 PROJECT SPECIFICATIONS

A.6.1 Backup

The solution must provide policy-driven, application-aware backups across all in-scope workloads with layered retention, immutable storage and verifiable restores. The complete in-scope system and workload register, including indicative vCPU, RAM and storage specifications, is set out in Section A.4 above.

Minimum requirements:

- **Schedules and retention:** daily incremental (14 days); weekly full (4 weeks); monthly full (12 months); annual full (5 years);
- **Application awareness:** VSS for Windows, database-consistent snapshots, and transaction-log handling where applicable, including for Microsoft SQL Server, Sage 300 People, Microsoft Dynamics GP and other line-of-business databases;

- **System State and configuration:** automated System State backups for all in-scope Windows servers, and configuration backups (including network device configuration, where applicable) for core NCR infrastructure;
- **User profiles:** backup and recovery of user profile data in accordance with NCR retention policy;
- **Security:** end-to-end encryption in transit and at rest; immutability / WORM; air-gapped or logically isolated copies; customer-managed keys preferred;
- **Quality and evidence:** automated monitoring and alerting, periodic test restores, and monthly backup reports covering success rate, capacity, trends and issues; and
- **Scalability:** capacity planning for at least 5% year-on-year growth, and the ability to onboard new servers and systems implemented during the contract period without re-architecture.

Bidder responses must include components, data flows, schedules, repositories, immutability design, key management, performance assumptions, restore processes and operational runbooks.

A.6.2 Disaster Recovery

The solution must provide orchestrated recovery to a South African cloud or physical DR site, enabling rapid failover and failback with minimal data loss and verified recovery processes. Minimum requirements:

- **Targets:** RPO of one (1) hour or less and RTO of four (4) hours or less for all in-scope systems;
- **Replication:** efficient host / virtual machine replication via direct connect, with dependency mapping and boot-order orchestration as needed;
- **Recovery methods:** support for bare-metal recovery, instant VM recovery, granular (file and item-level) recovery, and point-in-time recovery across all in-scope workloads;
- **Testing:** at least four (4) DR drills per year, each followed by a post-drill report covering gaps, lessons, improvements and recovery timing; and
- **Readiness:** DR dashboards, automated health checks, and control effectiveness evidence.

Bidder responses must include DR topology, replication schedules, orchestration tooling, failover and failback procedures, test methodology, performance assumptions and success criteria. Bidders must include the costing of four-hour quarterly DR drill resources where public cloud is proposed.

A.6.3 Implementation and Migration

- Bidders must own the end-to-end transition with minimal business disruption;
- A phased cutover plan is required: discovery, design, build, pilot, migration, stabilisation and optimisation;
- Pre-production testing of backup jobs, restores and DR runbooks is required;
- Responsible decommissioning of legacy backup infrastructure, with access to historical backup data retained for at least twelve (12) months unless directed otherwise; and
- A risk-based rollback plan is required for every milestone.

A.6.4 Network, Security and Compliance

- Residency: all data hosted within South Africa in Tier 3 or Tier 4 data centres (facilities to be declared with supporting evidence);
- Connectivity: 1 Gbps dedicated cross-connect plus a 100 Mbps IPSec VPN as a redundant path;
- Zero Trust: MFA / SSO, role-based access control, privileged access management, segmentation and micro-segmentation, and a secure bastion;
- Telemetry: daily monitoring and auditing of access and backup activities; and
- Remote access: fifteen (15) SSL VPN licences.

Bidders must provide a security architecture, a control map, and their approach to the compliance evidence pack.

A.6.5 Support and Service Management

- 24x7x365 service desk, ITIL-aligned (incident, request, problem and change management);
- A dedicated Project Manager and Infrastructure Architect, to be provided and costed;
- Monthly service reports covering backup KPIs, DR drill outcomes, security events and responses, capacity and growth, SLA performance, the risk register and continual service improvement actions; and
- Proactive monitoring with defined escalation paths.

A.6.6 Training and Certification

The bidder must deliver formal training and certify at least two (2) NCR engineers across configuration, recovery, monitoring, DR orchestration and security, including labs, materials and examinations where applicable.

A.6.7 Business Continuity Requirements

- The service must integrate with the NCR's business continuity management system (ISO 22301:2019);
- Bidders must supply and maintain DR runbooks, contact trees and service continuity plans, reviewed and tested quarterly;
- Impact-based restoration tiers and application dependency maps must be provided, with support for alternate access methods (for example secure client SSL VPN / VDI) during DR; and
- The solution must be embedded in NCR continuity governance and not operated as a standalone toolset.

A.7 NON-FUNCTIONAL REQUIREMENTS

- Availability: 99.9% for the backup control plane, with DR readiness dashboards available 24x7;
- Performance: consistent achievement of RPO and RTO targets;
- Scalability: at least 5% year-on-year growth without re-architecture;
- Reliability: at least 98% monthly backup success, with a restore failure rate of 1% or less (excluding corrupt sources);
- Security: Zero Trust controls, MFA, privileged access management, immutability, and ransomware detection and response; and
- Observability: end-to-end logging, metrics and dashboards.

A.8 ARCHITECTURE REQUIREMENTS

- A.8.1 Backup architecture: workload-aware backup proxies and agents; tiered repositories (performance plus immutable capacity) integrating with the NCR's internal immutable repository across its standalone Hyper-V hosts; object-lock / WORM for monthly and annual copies; an air-gap strategy; CMK / HSM-based key management; and validated restore paths (file, application, volume, bare-metal and virtual machine) supported by operational runbooks.
- A.8.2 DR architecture: replication from the primary on-premises environment (standalone Hyper-V hosts, not clustered) to a South African DR site via a 1 Gbps direct cross-connect, with a 100 Mbps IPSec VPN as backup; per-host near-synchronous replication; automated

orchestration (boot order, DNS updates and health checks); segmented DR landing zones with a secure bastion; SSO / MFA with break-glass controls (PAM); integrity-checked failback; and isolated bubble networks for non-disruptive testing.

- A.8.3 Network and security architecture: segregated management, backup, replication and tenant subnets; least-privilege ACLs; DDoS protections; DR-aware DNS with low TTLs; and QoS / throttling during business hours.

A.9 PROJECT MANAGEMENT AND PLANNING

- A.9.1 Governance and delivery: the bidder must follow a PRINCE2 / PMBOK-aligned delivery approach with agile configuration sprints; define a RACI between the NCR and the service provider across discovery, design, build, operations, DR drills and reporting; and operate an ITIL change advisory process with NCR approval gates.
- A.9.2 Indicative phased plan (12 weeks): mobilisation (week 1); discovery and assessment (weeks 1 to 2); high-level and low-level design and security design (weeks 3 to 4); build and configuration (weeks 5 to 7); pilot and testing (weeks 8 to 9); migration and cutover (week 10); and stabilisation and handover (weeks 11 to 12). Bidders may propose alternatives with explicit rationale; any change in RPO / RTO or risk posture must be highlighted.
- A.9.3 Milestones and deliverables: project charter and plan; HLD / LLD; security and key management plan; runbooks (backup, DR and failback); connectivity build book; test plans and results; cutover plan and go-live checklist; knowledge transfer and certification proof; operations handbook; and monthly reporting pack templates.
- A.9.4 Acceptance criteria: demonstrated RPO of one (1) hour or less and RTO of two (2) hours or less in pilot tests; at least 98% backup success over 30 consecutive days; a successful non-disruptive DR drill with documented recovery of critical services; and signed approvals on the HLD / LLD, runbooks and go-live checklist.
- A.9.5 Risk management: a maintained risk register with mitigations, addressing among others bandwidth constraints, seeding time, change freezes, ransomware scenarios, DR compute reservations, skills dependencies and certification expiries.
- A.9.6 Data migration, seeding and legacy retention: bidders must propose initial seeding (online versus bulk), timelines and chain of custody; maintain access to legacy backup data for at least twelve (12) months (or as directed); and document the retrieval method and cost.

A.10 SERVICE LEVELS (SLAs) AND REPORTING

A.10.1 Backup KPIs: backup job success rate of at least 98% monthly; restore request response within 30 minutes; restore initiation within 2 hours; integrity evidence per request; and monthly capacity forecasting and trend reports.

A.10.2 DR and continuity KPIs: quarterly DR drills (at least four per year) with post-drill reports within five (5) business days; RPO / RTO adherence of at least 99% for in-scope workloads; and an annual scenario-based test (for example ransomware or site failure).

A.10.3 Support SLAs (24x7x365): P1 (Critical): 15-minute acknowledgement, 1-hour workaround, 2-hour resolution target; P2 (High): 30-minute acknowledgement, 4-hour workaround, 8-hour resolution target; P3 (Medium): 1-hour acknowledgement, next-business-day resolution target; P4 (Low / Request): 4-hour acknowledgement, resolution within 3 business days.

A.11 MANDATORY COMPLIANCE AND ASSURANCE

- Proof that the proposed platform is POPIA compliant;
- Valid certificates for ISO 27001/27002:2022, ISO 22301:2019, ISO 27018:2019 and ISO 29151:2017;
- NIST Cybersecurity Framework control mapping for the proposed solution;
- South African Tier 3 or Tier 4 data centre certifications for the facilities used by the service; and
- Confirmation of security clearance eligibility of all directors and key personnel who will be exposed to sensitive NCR information, together with the personal particulars required for SSA vetting, to be submitted with the bid.

A.12 OPERATIONAL REQUIREMENTS

- Maintain current, version-controlled runbooks (backup restore, DR orchestration, failback, communications plan and decision matrix);
- Provide 24x7 monitoring of platform health, job status, capacity and anomalies; and
- Operate ITIL change windows (standard and emergency, via the NCR CAB), quarterly capacity reviews with a 12-month rolling forecast, vulnerability management, EDR on DR compute, threat intelligence integration, and log retention of at least twelve (12) months online with archival per policy.

A.13 GOVERNANCE AND REVIEWS

The NCR will convene monthly service reviews, quarterly executive reviews, and an annual roadmap session with the selected bidder.

A.14 ASSUMPTIONS AND CONSTRAINTS

- All data must remain within South Africa.
- The NCR will provide reasonable access to environments and subject matter experts for discovery and testing; and
- Scope changes follow formal change control, and all third-party costs must be disclosed.

A.15 FINANCIAL / PRICING REQUIREMENTS

- All pricing must be inclusive of VAT;
- Pricing must be in South African Rand, even where a Rand / Dollar exchange rate applies to software licences; and
- Pricing must include annual escalations where applicable.

Note: no pricing or costing variations will be entertained after the conclusion of the SLA / contract (or after the appointment).

A.16 FUNCTIONAL EVALUATION

Bidders' proposals will be scored according to the following rating scale: **0 = no or irrelevant submission; 1 = poor; 2 = does not meet the requirements; 3 = partially meets the requirements; 4 = meets the requirements; 5 = exceeds the requirements.**

Functional Evaluation Criteria	Scoring Criteria (0 to 5 Rating)	Weight
1. Bidder's Technical Approach: executive summary; understanding of the requirements; technical solution; detailed architectures (backup, DR, network and security); data migration and seeding plan; project plan and method; security and compliance; risks and mitigations; service management; and training plan.	5 = Meets all elements; 4 = Meets six elements; 3 = Meets four elements; 2 = Meets two elements; 1 = Meets one element; 0 = Does not meet any element.	40%
2. Bidder's Experience / Reference Letters: contactable reference letters confirming successful delivery of backup and DR projects on public cloud or private hosting environments within the last five (5) years.	5 = Five or more letters; 4 = Four letters; 3 = Three letters; 2 = Two letters; 1 = One letter; 0 = No letters submitted.	30%

Functional Evaluation Criteria	Scoring Criteria (0 to 5 Rating)	Weight
3. Project Manager: CV of a Project Manager (10+ years' experience) demonstrating active participation in successfully delivered cloud or private hosting migration projects.	5 = Five projects; 4 = Four projects; 3 = Three projects; 2 = Two projects; 1 = One project; 0 = No CV attached or no relevant projects demonstrated.	10%
4. Infrastructure Architect: CV of an Infrastructure / Solution Architect (10+ years' experience) demonstrating active participation in similar cloud or private hosting migration projects.	5 = Five projects demonstrated; 4 = Four projects; 3 = Three projects; 2 = Two projects; 1 = One project; 0 = No CV attached or no relevant projects demonstrated.	10%
5. Supporting Engineers: CVs of other cloud / private infrastructure engineers (10+ years' experience) demonstrating active participation in similar projects.	5 = Five projects; 4 = Four projects; 3 = Three projects; 2 = Two projects; 1 = One project; 0 = No CVs attached or no relevant projects demonstrated.	10%
TOTAL		100%

Important note to bidders: the schedules referenced in these Terms of Reference must be fully completed as provided. Non-compliance with this requirement on any item in the schedules will lead to disqualification of the bid. Bidders must score a minimum of 80% on functionality to be eligible for the price and specific goals evaluation.

A.17 PRICING SCHEDULE

Option A: Public Cloud

Once-off DR implementation charges (non-recurring):

No.	Item Description	Total Price (VAT incl.)
1.	Backup and DR design and implementation	
2.	DR testing and implementation	
3.	Project Manager per hour cost (12 weeks, 160 hours per month)	
4.	Training and certification	
5.	Other charges (itemised)	
TOTAL		

Recurring charges (all items):

Item Description	Year 1	Year 2	Year 3
Backup and DR licences			
Public cloud costs covering all elements of the TOR			
Supporting onsite Infrastructure Architect (10+ years' experience) per hour, 160 hours per month			
TOTAL			

Grand total:

Total Cost	36 Months
Total non-recurring cost (once off)	
Total recurring cost	
VAT 15%	
GRAND TOTAL	

Option B: Private Hosting

Once-off DR implementation charges (non-recurring):

No.	Item Description	Total Price (VAT incl.)
1.	Backup and DR design and implementation	
2.	DR testing and implementation	
3.	Project Manager per hour cost (12 weeks, 160 hours per month)	
4.	Training and certification	
5.	Other charges (itemised)	
TOTAL		

Recurring charges (all items):

Item Description	Year 1	Year 2	Year 3
Backup and DR licences			
Physical hardware and Hyper-V licence costs covering all elements of the TOR			
Supporting onsite Infrastructure Architect (10+ years' experience) per hour, 160 hours per month			
TOTAL			

Grand total:

Total Cost	36 Months
Total non-recurring cost (once off)	
Total recurring cost	
VAT 15%	
GRAND TOTAL	

A.18 BID RESPONSE SCHEDULES

Bidders must complete the following schedules in full, in line with the submitted reference letters and CVs. The NCR reserves the right to contact the listed references for verification purposes.

- **Schedule B:** Company experience, listing the institution, project description, project start and end dates, reference name, telephone number and email address for each reference;

- **Schedule C:** Pool of project resources, listing each team member, their role in the project (Project / Account Manager, Solution / Infrastructure Architect, or other consultant) and their qualifications, with copies of qualifications attached; and
- **Schedule D:** Project Manager's and Solution / Infrastructure Architect's experience, listing the institution, project description, project dates and reference contact details for each cited project.

- ANNEXURE_B: COMPANY EXPERIENCE
- SCHEDULE OF COMPANY'S EXPERIENCE: LIST OF REFERENCES
- COMPANY NAME: _____

No.	Name of Institution	Project Description	Project Start Date (dd/mm/yyyy)	Project End Date (dd/mm/yyyy)	Name of Reference	Contacts Details of Reference	
						Telephone No.	Email Address
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

- This must be in line with the provided / submitted Reference Letters: NB.: NCR reserves the right to contact the listed contact for verification purposes
- ANNEXURE_C: POOL OF PROJECT RESOURCES

-
- **SCHEDULE OF POOL OF PROJECT TEAM / RESOURCES:**

No.	Name of Project Resource / Team Member	Role in the Project (Project / Account Manager / Solution's/ Infrastructure Architect (and / or other Consultant, etc.)	List of Qualifications per Resource
1			
2			
3			
4			
5			
6			
7			

- **Note: Please attach the copy of qualifications per resource as specified on this table**

-
-
-

- ANNEXURE_D: PROJECT / ACCOUNT MANAGER'S EXPERIENCE

-

- LIST OF REFERENCES

- E-1: PROJECT MANAGER'S NAME: _____

No.	Name of Institution	Project Description	Project Start Date (dd/mm/yyyy)	Project End Date (dd/mm/yyyy)	Name of Reference	Contacts Details of Reference	
						Telephone No.	Email Address
1							
2							
3							
4							
5							
6							

-

-

-

-

-

-

- D-2: SOLUTION/INFRASTRUCTURE ARCHITECT'S NAME: _____

No	Name of Institution	Project Description	Project Start Date (dd/mm/yyyy)	Project End Date (dd/mm/yyyy)	Name of Reference	Contacts Details of Reference	
						Telephone No.	Email Address
1							
2							
3							
4							
5							
6							

- This must be in line with the provided / submitted CV's
- NB.: NCR reserves the right to contact the listed contact for verification purposes
-

END of document