THE NATIONAL CREDIT REGULATOR

OCTOBER 2026

TERMS OF REFERENCE FOR THE APPOINTMENT OF A SUITABLY QUALIFIED SERVICE PROVIDER TO SUPPLY, CONFIGURE, IMPLEMENT, INTEGRATE, MIGRATE, TRAIN, SUPPORT AND MAINTAIN AN INTEGRATED REGULATORY INFORMATION MANAGEMENT SYSTEM (IRIS).

RFP NUMBER: NCR1056.11.2026

Compulsory briefing session
Date: 13 November 2026
Time: 10H00 am to 11H00am
Venue: Online MS Teams
Link below:

Microsoft Teams meeting
Join: https://teams.microsoft.com/meet/354767111564689?p=y9wsswSi40W2H264dU
Meeting ID: 354 767 111 564 689 2
Passcode: LW6ad3f2

DUE DATE: 07 DECEMBER 2026 AT 11H00 SHARP CAT
ADDRESS: 127-15TH ROAD RANDJESPARK 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 **07 December 2026** and must be enclosed in a sealed envelope which must be clearly labelled/addressed on the outside.

a) RFP No: NCR1056.11.2026

b) TERMS OF REFERENCE FOR THE APPOINTMENT OF A SUITABLY QUALIFIED SERVICE PROVIDER TO SUPPLY, CONFIGURE, IMPLEMENT, INTEGRATE, MIGRATE, TRAIN, SUPPORT AND MAINTAIN AN INTEGRATED REGULATORY INFORMATION MANAGEMENT SYSTEM (IRIS).

c) CLOSING DATE: 07 DECEMBER 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 am** on **07 December 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
05/11/2026	Issue RFQ document
13/11/2026	Compulsory Briefing Session
07/12/2026	Closing date
08/12/2026	Preliminary evaluation
08/12/2026	Evaluations by the Evaluation Committee
25/01/2027	Adjudication Committee meeting
01/02/2027	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/procument/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
Persons historically disadvantaged based on age	50%- 100% owned by persons who are youth	3
	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: NATIONAL CREDIT REGULATOR TERMS OF REFERENCE: APPOINTMENT OF A SERVICE PROVIDER TO SUPPLY, CONFIGURE, IMPLEMENT, INTEGRATE, MIGRATE, TRAIN, SUPPORT AND MAINTAIN A REGULATORY INFORMATION MANAGEMENT SYSTEM (IRIS)

Delivery model	Configurable commercial off-the-shelf (COTS) or established low-code platform, delivered as SaaS
Mandatory MVP deadline	Production-usable MVP accepted by NCR no later than the end of Month 6 from project commencement
Full solution delivery	Remaining contracted scope delivered in subsequent NCR-approved phases following MVP acceptance, in accordance with the accepted implementation plan
Contract term	Initial 3 years, with an NCR option to extend for up to a further 2 years
Primary outcome	One integrated platform spanning registration, payment, verification, complaints/disciplinary management, reporting and auditability

1. 1. Background

The National Credit Regulator (NCR) is responsible for the registration, regulation and oversight of credit providers, credit bureaus, credit bureau resellers and debt counsellors in South Africa. The NCR requires reliable, consistent and auditable information to administer registrations, payments, complaints, investigations, decisions and public verification of regulated entities.

Current processes rely, to varying degrees, on manual activities, spreadsheets and/or legacy systems. This creates administrative burden, fragmented information, inconsistent turnaround times, limited end-to-end visibility and difficulty providing timely self-service to applicants, registrants and members of the public.

The NCR therefore intends to procure an integrated Regulatory Information Management System (IRIS) that digitises the regulatory lifecycle, consolidates entity and case information, improves operational control and reporting, and provides secure public-facing self-service capabilities.

2. 2. Purpose and Objectives

1. 2.1 Purpose

The purpose of this Terms of Reference is to invite suitably qualified and experienced service providers to supply, configure, implement, integrate, migrate data to, train users on, support and maintain a configurable COTS or established low-code IRIS delivered as Software-as-a-Service (SaaS).

Overarching security obligation: The service provider must propose, supply, configure, implement, test, evidence, operate, monitor, maintain and continuously improve proportionate security and privacy measures throughout the full service lifecycle. Security must be embedded in the bidder's solution architecture, implementation methodology, project plan, resourcing, pricing, risk approach, testing, acceptance, support, subcontractor management and exit arrangements, and may not be treated as an optional item or deferred activity.

2. *2.2 Objectives*

- Implement one integrated workflow platform covering the full regulatory lifecycle, with a single entity master record, shared document repository, common activity timeline and central audit trail.
- Provide secure digital self-service for applications, supporting documents, payments, verification and complaints.
- Automate submission screening, work allocation, approvals, notifications, renewals, escalations and status changes through configurable rules and workflows.
- Enable NCR business and ICT administrators to maintain fields, forms, statuses, rules, fee tables, templates, workflows and reports using standard configuration tools without changing vendor core source code.
- Improve transparency, operational reporting, management information, turnaround monitoring and regulatory insight.
- Protect NCR information through appropriate identity, security, privacy, retention, backup and disaster recovery controls.
- Ensure NCR retains ownership and practical portability of its data, metadata, documents, audit logs and configurations.
- Deliver measurable business value early through a mandatory production-usable MVP within the first six months of the project.

3. 3. Guiding Principles

Configuration over custom development: The proposed solution must be a proven commercial product or established low-code platform. Core functionality must be delivered primarily through standard product capability and configuration. Greenfield custom development is not acceptable.

One integrated regulatory platform: Separate business modules may serve different teams, but they must operate on common entity, document, workflow, timeline and audit foundations. Manual transfer between unrelated point solutions is not acceptable.

NCR extensibility: NCR-authorised administrators must be able to make routine configuration changes after go-live without vendor dependence.

MVP first: The implementation must prioritise a usable end-to-end registration and verification service that can be accepted and used in production by the end of Month 6.

Security and privacy by design: POPIA, least-privilege access, auditability, secure integration, encryption, resilient hosting and tested recovery must be built into the service.

Sustainable total cost: The solution must remain affordable, supportable, scalable and upgradeable for the full contract lifecycle. Hidden dependencies and unquoted recurring costs are not acceptable.

NCR owns its information: All NCR data and generated records remain NCR property and must be exportable in documented, non-proprietary formats.

Adoption and skills transfer: Implementation is not complete until users are trained, administrators can perform agreed routine configuration independently, and support/handover arrangements are operational.

4. 4. NCR Core Mandate and Core Business Summary

The NCR is established under the National Credit Act, 34 of 2005, to regulate South Africa's consumer credit market, protect consumers and promote a fair, transparent, competitive, sustainable, responsible, efficient, effective and accessible credit industry. Its core mandate is delivered through the following integrated business functions, which the IRIS solution must support with reliable information, controlled workflows, public access, regulatory oversight and auditable decision-making.

Core mandate / business function	Summary of NCR responsibility	IRIS business support required
Registration and industry entry control	Register and maintain regulatory records for credit providers, credit bureaux, credit bureau resellers, debt counsellors, payment distribution agents and other persons or entities required to register under the National Credit Act and applicable regulations.	Digital applications, validation, fee processing, assessment, approvals, certificates, conditions, renewals, amendments, suspensions, cancellations, status history and a reliable entity master record.
Compliance monitoring and supervision	Monitor the conduct and ongoing compliance of registrants with the Act, regulations, registration conditions, prescribed standards and lawful information-submission requirements.	Compliance returns, monitoring plans, risk indicators, inspections, findings, remedial actions, deadlines, evidence, escalation and management reporting.
Complaints, investigations and enforcement	Receive and assess complaints, investigate alleged contraventions, promote appropriate informal resolution, issue or pursue corrective measures, and refer matters to the National Consumer Tribunal or other competent authorities where required.	Omnichannel complaint intake, case triage, investigation workflows, evidence and correspondence management, confidential records, outcomes, referrals, enforcement actions, status impacts and complete audit trails.
Consumer protection, education and awareness	Protect consumer rights and improve public understanding of responsible borrowing, credit information, debt counselling, over-indebtedness, prohibited conduct and remedies available under the Act.	Accessible public information, self-service enquiries and complaints, consumer guidance, notifications, campaign records, stakeholder engagement information and reliable public verification services.
Credit-market research and monitoring	Research and monitor the consumer credit market, including access to credit, cost of credit, market conduct, credit information, indebtedness, trends and factors affecting competition or consumer protection.	Structured regulatory data collection, data-quality controls, dashboards, trend analysis, scheduled and ad hoc reports, secure data extracts and integration with approved analytical tools.
Policy, legislative and regulatory advice	Advise government and relevant authorities on consumer-credit policy, legislation, market developments, systemic risks and regulatory interventions informed by evidence and operational experience.	Trustworthy management information, research datasets, consolidated case and compliance insights, decision records and reproducible reports.
Stakeholder and regulatory coordination	Cooperate with the National Consumer Tribunal, government departments, law-enforcement bodies, other regulators, industry participants and consumer stakeholders to support consistent regulation and enforcement.	Controlled referrals, secure information exchange, meeting and decision records, role-based access, integration capability and traceable inter-agency correspondence.
Regulatory information	Maintain accurate regulatory records, protect personal and confidential information, provide authorised access to public register information,	Data ownership, records retention, POPIA-aligned controls, security, auditability, public registers, operational and statutory reporting,

governance and public accountability	support statutory reporting and demonstrate fair, consistent and accountable administration.	availability, backup, disaster recovery and data portability.

5. Contract Term and Delivery Model

The initial contract term will be three (3) years from the effective date, with an option exercisable solely by NCR to extend the contract for up to a further two (2) years. Any extension will be subject to satisfactory performance against contracted service levels and deliverables, continued business need, budget availability and applicable NCR governance and procurement requirements.

The service shall be delivered as SaaS, with hosting, infrastructure, platform maintenance, security patching, backups, disaster recovery and vendor-managed product upgrades included in the contracted service unless explicitly identified and priced otherwise.

6. Scope of Work

1. 6.1 Integrated Functional Modules

Ref	Module	Minimum capability
M1	Entity and account management	One master record per registered or non-registered entity; contacts, related parties, branches, registrations, status history, duplicate detection and controlled merge.
M2	Applicant / registrant self-service and application intake	Mobile-responsive portal; configurable application types and forms; save/resume; structured data and document upload; acknowledgements and reference numbers.
M3	Automated submission screening	Configurable completeness/compliance rules; validation of mandatory fields, document types and validity dates; automatic deficiency notices.
M4	Pricing, payment and financial integration	Effective-dated fee tables and fee rules; sales-order generation; payment initiation; invoice/payment/receipt status integration with the NCR Financial System; reconciliation reporting. The NCR financial platform remains system of record for accounting transactions.
M5	Administrative screening and work management	Queues, assignment, checklists, escalation, workload visibility and turnaround timers.
M6	Application review and approval	Reviewer assignment, configurable checklists, requests for additional information, clock-stop/restart, recommendations, peer review and multi-level approvals.
M7	Advisory committee / meeting management	Agenda compilation, meeting packs, attendance and declarations, resolutions, and write-back of outcomes to applications.
M8	Registration and certificate lifecycle	Registration/certificate issue with conditions and unique number; renewals, amendments, suspensions, cancellation/deregistration, reinstatement and complete status history.
M9	Public register and verification	No-login public search; display of approved public registration information and current status; clear suspended/deregistered indicators; verifiable certificate or digital card with QR code linking to the live register entry.
M10	Complaints, investigations and enforcement case management	Public complaint intake with evidence; registered and non-registered entities; categorisation, screening, investigation, outcome/closure stages; confidential notes;

		status impacts; complainant progress checking; turnaround and trend reporting. Allow complaints to submission via calls, emails or web portal.
M11	Activity timeline, correspondence, documents and audit	Single chronological entity view across applications, decisions, payments, complaints, correspondence and documents; templated outbound correspondence; tamper-evident searchable/exportable audit logs recording create, view, change and delete actions.
M12	Reporting and analytics	Dashboards and reports for volumes, renewals, payments/revenue, backlogs, turnaround, complaints and trends; scheduled reports; Excel/CSV export; configurable report builder; API and/or Power BI integration capability.

2. 6.2 Configuration and Maintainability

Configuration of NCR processes must use supported platform tools for workflows, forms, fields, statuses, rules, roles, templates, fee tables, notifications and reports. Changes to the vendor core product source code are not permitted. Any bidder-proposed custom extension must be clearly identified, justified, separately priced, supported through upgrades and approved by NCR before implementation.

3. 6.3 Integrations

- Two-way integration with the NCR Financial System using documented and secure APIs for sales orders/invoicing and return of invoice, payment and receipt status.
- Integration with a South African payment gateway supporting card, EFT and/or instant EFT as agreed by NCR.
- Integration with NCR identity services for single sign-on and multi-factor authentication for internal users.
- Integration with email and SMS notification services.
- Integration and/or secure publishing mechanism for the NCR website/public register.
- Documented standards-based REST APIs for future integration with other NCR or external systems and for controlled data export/reporting.

4. 6.4 Data Migration

- Migration of agreed legacy records, active and historical registrations, payment history, relevant documents, open applications and open complaints/cases.
- Data profiling, cleansing support, mapping, de-duplication, trial migrations, reconciliation and exception management.
- Defined cut-over strategy, rollback provisions and NCR sign-off before production migration.
- For the MVP, priority migration must at minimum make active registrants, current registration status, open applications and other data specifically agreed for the MVP available in the production solution. The remaining approved historical data must be migrated by full go-live unless NCR approves a different migration wave.

5. 6.5 Training, Adoption and Skills Transfer

- Role-based end-user training for administrators, reviewers, investigators, finance users, managers and other agreed user groups.
- Train-the-trainer sessions and reusable user guides, quick-reference guides and recorded training content.
- Public/applicant guidance appropriate to the self-service portal, including short user guides or videos where required.

- An adoption and communications plan covering readiness, stakeholder communication, launch support and transition into business-as-usual.
- Structured skills transfer enabling nominated NCR ICT/business administrators to manage users, roles, fee tables, templates, reports and agreed simple workflow/form changes without routine vendor intervention.
- Administrator certification or equivalent vendor/platform accreditation for nominated NCR personnel where available.

7. 7. Mandatory MVP and Implementation Roadmap

1. *7.1 MVP Deadline*

The service provider must deliver an NCR-accepted, production-usable Minimum Viable Product (MVP) no later than the end of Month 6 from the agreed project commencement date. The MVP deadline is a mandatory contractual milestone and must be reflected in the bidder's project plan, resource plan, pricing and risk management approach.

An MVP will not be accepted if it is limited to a prototype, design, proof of concept, demonstration, partially configured sandbox or test environment. Acceptance requires the agreed MVP scope to be deployed in production and capable of supporting real NCR users and transactions, subject to NCR go-live approval.

2. *7.2 Minimum MVP Scope*

Ref	MVP requirement	Priority
MVP-01	Secure production SaaS environment, SSO/MFA, role-based access and baseline security controls	Mandatory
MVP-02	Core entity master with registered/non-registered entity records, duplicate controls and status history	Mandatory
MVP-03	Mobile-responsive applicant/registrant portal with agreed priority application forms, save/resume and document upload	Mandatory
MVP-04	Automated completeness checks, acknowledgements, reference numbers and deficiency notifications	Mandatory
MVP-05	Administrative screening, work queues, review workflow, additional-information cycle and approval decision	Mandatory
MVP-06	Configurable fee calculation and agreed payment / NCR Financial System integration sufficient for the priority registration process	Mandatory
MVP-07	Registration/certificate issuance, agreed renewal/status controls and complete activity history for MVP transactions	Mandatory
MVP-08	Public register search and verification of approved public fields and current registration status	Mandatory
MVP-09	Email/SMS notifications for agreed priority events	Mandatory
MVP-10	Tamper-evident audit trail and core operational dashboards/reports	Mandatory
MVP-11	Priority data migration and reconciliation for agreed active/current records	Mandatory
MVP-12	UAT completion, user/admin training, operating procedures, support readiness and production handover for MVP scope	Mandatory

3. *7.3 MVP Acceptance Gate*

- All MVP requirements are linked to tested configurations and have been accepted by NCR business and ICT representatives.

- User acceptance testing has been completed against approved test scenarios and NCR has issued written acceptance or a conditional acceptance that does not prevent safe production use.
- No open Severity 1 or Severity 2 defect exists at go-live; any lower-severity accepted defects have agreed remediation dates.
- Production identity/access controls, logging, backups and recovery arrangements are active and evidenced.
- The service provider has implemented and evidenced all security measures committed in its proposal and required by NCR; security testing and remediation are complete; there are no open critical or high-risk vulnerabilities unless NCR has formally accepted the residual risk in writing.
- MVP integrations required for live processing have successfully completed agreed end-to-end tests.
- Priority migrated data has been reconciled to agreed totals/controls and signed off by NCR.
- MVP users and administrators have received the agreed training and support channels are operational.
- Go-live, rollback, support and incident escalation procedures have been approved.

4. 7.4 Phased Implementation

Phase	Timing	Required outcome
Mobilisation & design	Weeks 1-4	Project mobilisation; confirmed scope/backlog; solution design; configuration catalogue; integration and migration design; security plan; detailed delivery plan and acceptance plan.
MVP build & configuration	Months 1-4	Configure the priority end-to-end registration service, MVP integrations, trial migration, technical testing, training preparation and change/adoption activities.
MVP integration, UAT & production go-live	Months 4–6	Complete integration testing, migration rehearsal, UAT, remediation, production cut-over and NCR acceptance. The MVP must be accepted no later than the end of Month 6.
Post-MVP full-scope implementation	From Month 7	Complete the remaining contracted modules and capabilities, including complaints/disciplinary management, committee workflows, advanced reporting, remaining migration and integrations; optimize configuration based on MVP use.
Full go-live & transition	As per approved full implementation plan	Full-scope UAT/sign-off, final production release, remaining migration, knowledge transfer and transition to support.
Hypercare	3 months after full go-live	Enhanced support, defect remediation, adoption monitoring, performance review and operational stabilisation.

Bidders may propose a faster delivery plan, but may not move the MVP milestone beyond the end of Month 6 without explicit NCR approval. Post-MVP implementation milestones must be clearly defined in the bidder's project plan and, once approved by NCR, may not be changed without formal change control. Delays attributable to supplier resourcing, product readiness or subcontractors will not constitute grounds for automatic milestone extension.

8. Technical, Security and Non-Functional Requirements

Ref	Area	Requirement
NFR-01	Architecture	Cloud-hosted SaaS with logical segregation of NCR data and supported environments for development/configuration, test/UAT and production.
NFR-02	Availability	Minimum 99.5% monthly service availability, excluding agreed maintenance windows.
NFR-03	Identity	Single sign-on with the NCR identity provider and multi-factor authentication for all internal users.
NFR-04	Access control	Role-based access at module, action and where required record level; least privilege and separation of duties.
NFR-05	Privacy	POPIA-aligned processing, consent and access controls where applicable, retention rules, and disclosure of hosting locations/sub-processors/cross-border transfers.
NFR-06	Security assurance	The service provider must provide and implement a documented information-security management approach covering governance, secure design and configuration, threat and risk assessment, vulnerability and patch management, secure development/change control, malware protection, monitoring, incident response, personnel and subcontractor controls, and continuous improvement. Independent security assurance such as ISO/IEC 27001 certification or SOC 2 Type II must be provided, together with annual independent penetration testing and agreed results/evidence made available to NCR. Identified vulnerabilities must be risk-rated, remediated within NCR-approved timeframes and verified before closure.
NFR-07	Encryption	Encryption of NCR data in transit and at rest using current industry-standard cryptography.
NFR-08	Backup and DR	Daily or better backups and documented disaster recovery with stated and contractually committed RPO and RTO.
NFR-09	Auditability	Tamper-evident audit logs for material user/system actions, searchable and exportable by authorised NCR users.
NFR-10	Retention	Configurable record retention/disposal rules aligned to the NCR file plan and applicable records-management obligations.
NFR-11	APIs	Documented secure APIs for required integrations and controlled data export.
NFR-12	Accessibility	Public-facing portal must be mobile responsive and target WCAG 2.1 AA accessibility.
NFR-13	Scalability	Ability to support growth in registrants, applications, documents, complaints, users and transaction volumes without reimplementation.
NFR-14	Performance	Bidder to propose measurable response-time targets for key interactive transactions and reports and demonstrate capacity for expected workload.
NFR-15	Maintainability	Vendor-managed upgrades must preserve supported configurations and agreed integrations; release notes and impact assessments must be supplied.
NFR-16	Data portability	NCR data, documents, metadata, audit records and configurations must be exportable in documented, usable and non-proprietary formats.

9. 9. Project Governance and Delivery Management

- The service provider must appoint a suitably experienced Project Manager as the single accountable delivery lead.
- A joint project governance structure must be established at mobilisation, including project/steering meetings, workstream leads, decision paths, issue and risk escalation, and reporting cadence.
- The service provider must maintain an integrated project plan, RAID log, dependency log, decision log, requirements traceability matrix, test/defect register and change register.
- Weekly implementation status reporting is required through full go-live, covering progress against milestones, budget, risks, issues, dependencies, decisions, resource status and next-period activities.
- All changes to approved scope, schedule or cost must follow formal change control and require NCR approval before implementation.
- The service provider remains accountable for subcontractors, platform vendors and implementation partners used to deliver the service.

10. 10. Deliverables and Acceptance

Ref	Deliverable	Due	Acceptance basis
D1	Mobilisation pack and detailed project plan	Within 10 business days of commencement	Approved governance, schedule, resource plan, RAID/dependency logs and delivery controls.
D2	Solution design and requirements traceability matrix	Month 1	Approved functional/technical design, configuration catalogue, integration and migration design, proposal-specific security and privacy plan, security architecture and data flows, control matrix, implementation schedule, threat/risk assessment and requirements traceability.
D3	MVP configured in test/UAT	During Months 1 - 5	MVP scope available for structured testing with agreed test data and test evidence.
D4	MVP production release	No later than end Month 6	All MVP acceptance-gate criteria met and NCR production go-live/acceptance issued. **Security acceptance condition:** NCR may withhold release, go-live or deliverable acceptance where required security controls have not been implemented and evidenced, material vulnerabilities remain unresolved, or the service provider has not complied with the approved security and privacy plan.
D5	Full configured solution	In accordance with the NCR-approved post-MVP implementation plan	All contracted modules/configuration completed and accepted, subject to approved phased backlog.
D6	Data migration and reconciliation	MVP priority set by Month 6; remaining	Reconciled migrated data, exception report and NCR sign-off.

		agreed set by full go-live	
D7	Integrations	MVP-priority integrations by Month 6; remaining by full go-live	End-to-end tested interfaces, technical documentation and operational monitoring.
D8	Testing and quality pack	Per release	Test strategy/scripts, results, defect register, NCR UAT sign-off and security evidence for every release, including secure-configuration review, access-control testing, vulnerability scanning, penetration testing where applicable, remediation verification, logging/monitoring validation, backup/restore testing and confirmation that no unacceptable security exposure remains.
D9	Training and adoption pack	Before each production release	Training plan, manuals, quick guides, recorded sessions where agreed, attendance/completion evidence and adoption support.
D10	Go-live and support readiness pack	Before each go-live	Cut-over, rollback, support model, escalation matrix, DR/backup evidence and operational handover.
D11	Skills transfer completion report	By end of full-go-live hypercare	Evidence that nominated NCR staff can perform agreed routine administration/configuration independently.
D12	Monthly service and usage report	Monthly during support term	SLA performance, incidents, problems, availability, security/patch status, usage, capacity, changes/releases and service improvement actions.
D13	Exit and transition pack	On expiry/termination or when requested under exit provisions	Data export, documentation, knowledge transfer, transition assistance and deletion certification after NCR confirmation.

NCR acceptance will be in writing. Payment milestones should, where practical, be linked to accepted deliverables rather than elapsed time alone. Acceptance does not waive latent defects, security obligations, data integrity requirements or warranty/support obligations.

11. 11. Support, Maintenance and Service Levels

1. 11.1 Support Model

- Local South African first-line support during NCR business hours, with defined escalation to specialist/vendor support.
- Vendor-managed platform upgrades, security patches, and corrective maintenance included in the subscription/support service.
- Continuous security operations must include monitoring and alerting, privileged-access review, vulnerability scanning, patching, secure configuration management, incident and breach response, backup verification, periodic recovery testing, annual independent penetration testing, remediation tracking and monthly security-status reporting to NCR.
- A documented service desk process, escalation matrix, incident/problem management process and planned maintenance notification process.

- Refresher training and release-impact communication after material platform releases where functionality or user processes change.

2. *11.2 Minimum Service Level Proposal*

Bidders must propose measurable service levels that meet or improve the following baseline. Final values will be agreed during contracting and incorporated into the SLA.

Measure	Definition	Minimum expectation
Availability	Production service availability	≥ 99.5% per calendar month, excluding approved maintenance
Severity 1	Critical outage/security event with material business impact	Immediate logging and escalation; bidder to propose rapid response and restoration targets with 24x7 escalation capability for critical incidents
Severity 2	Major degradation or major function unavailable	Bidder to propose response/restoration targets suitable for business-critical regulatory operations
Severity 3/4	Moderate/minor defects or service requests	Defined business-hours response and resolution targets
DR	Recovery Point Objective / Recovery Time Objective	Bidder to state committed RPO/RTO and test recovery at least annually
Reporting	Service performance report	Monthly
SLA failure	Service credits and corrective action	Defined service credits plus root-cause/corrective-action plan for repeated or material failures

12. Data Ownership, Records and Exit

- All NCR data, documents, metadata, audit logs and NCR-specific configurations remain the property of NCR.
- The service provider may process NCR information only for the contracted purpose and must comply with approved security, privacy, retention and deletion requirements.
- NCR must be able to export its data during the contract in documented formats without loss of material meaning or relationships.
- On expiry or termination, the service provider must return all NCR data, documents and audit logs in a documented, non-proprietary format within 30 days or another period agreed in the contract, provide reasonable transition assistance, and certify deletion after NCR confirms successful handover and retention requirements.
- Bidders must disclose whether source-code escrow or equivalent continuity arrangements are available and any associated cost. NCR ownership of vendor core source code is not required.

13. 13. Mandatory Bidder and Solution Requirements

Bids that fail a mandatory requirement may be regarded as non-responsive and excluded from further functionality evaluation, subject to NCR SCM rules and the final bid conditions.

Ref	Requirement	Minimum condition	Evidence
MR1	Solution maturity	The proposed platform must be commercially available / established and already in live production or implementation	Signed reference letters or verifiable client references

		at a minimum of three (3) reference sites, of which at least two (2) should be regulatory, oversight, professional or membership bodies with materially comparable processes.	showing modules, go-live/implementation status and contact details.
MR2	No greenfield custom build	Core scope must be delivered through standard functionality and configuration on the proposed product/platform.	Product description, architecture and completed compliance matrix.
MR3	MVP commitment	Bidder must commit to NCR acceptance of the production-usable MVP no later than the end of Month 6.	Signed implementation commitment plus detailed project plan, resources, dependencies, and MVP acceptance approach.
MR4	Local presence/support	Bidder must be registered in South Africa or have a South African implementation/support partner accountable for the full contract term.	CIPC/CSD details and, where applicable, signed partnership/subcontracting agreement.
MR5	Support and maintenance	Full support, maintenance, security patching and vendor-managed upgrades for the contract term.	Support model, SLA proposal and escalation matrix.
MR6	Training and skills transfer	Comprehensive role-based training, administrator/configuration documentation and structured skills transfer.	Sample materials and proposed training/skills-transfer plan.
MR7	POPIA and security	The bidder must provide a complete security and privacy proposal and commit to implementing, operating, monitoring, maintaining and improving the specified controls throughout mobilisation, design, configuration, integration, migration, testing, go-live, support and exit. The response must address at minimum security governance, POPIA, hosting and data location, identity and privileged access, encryption and key management, secure APIs, vulnerability and patch management, logging and monitoring, incident and breach response, backups and recovery, personnel security, subcontractors/sub-processors, secure deletion and independent assurance. Material exceptions or deferred controls are not acceptable unless expressly approved by NCR.	A proposal-specific security and privacy plan; control matrix mapped to Section 8; solution and data-flow architecture; security implementation schedule with accountable resources; hosting and sub-processor details; certifications and independent assurance reports; recent penetration-test summary and remediation status; vulnerability, patch, incident-response, backup/DR and secure-exit procedures; and confirmation that all mandatory security costs are included in the bid price.
MR8	Tax and supplier compliance	Bidder must meet applicable SARS tax-compliance and Central Supplier Database requirements.	Valid evidence as required in the bid invitation.

1. *13.1 Key Project Team*

Bidders must identify the proposed key personnel and provide CVs demonstrating relevant qualifications, platform experience and comparable delivery experience. At minimum, the team must cover: Project Manager, Solution Architect, Business/Process Analysis, Configuration Lead, Integration Lead, Data Migration Lead, Testing/Quality Lead, Security Lead and Training/Change Lead. One person may cover more than one role only where the bidder demonstrates that delivery capacity and segregation of responsibilities will not be compromised.

14. 14. Bid Submission Requirements

1. Solution description and architecture, including hosting model, product version, release cadence and product roadmap.
2. Completed functional requirements compliance matrix using the response codes in Section 19.
3. Detailed implementation methodology phased project plan and resourcing plan explicitly demonstrating delivery of the MVP by end of Month 6, together with a credible post-MVP roadmap and milestones for completion of the remaining contracted scope.
4. MVP definition and traceability showing how each mandatory MVP requirement will be delivered, tested and accepted.
5. Data migration methodology and indicative migration assumptions.
6. Integration approach and API capabilities.
7. A proposal-specific security and privacy response setting out the security measures the bidder will provide and implement throughout the lifecycle, including a Section 8 control matrix, security architecture and data flows, implementation activities and milestones, accountable Security Lead and resources, hosting/sub-processors, POPIA controls, secure integration and migration, identity and privileged access, encryption, vulnerability and patch management, monitoring, incident response, backup/disaster recovery, security testing, independent assurance, remediation, support and secure exit.
8. Support model, proposed SLA, service-desk arrangements and escalation matrix.
9. Training, adoption and skills-transfer approach.
10. Risks, assumptions and dependencies, clearly distinguishing supplier-controlled and NCR-controlled dependencies.
11. Client references and CVs of key personnel.
12. Pricing schedules and total cost of ownership for the maximum five-year period, with assumptions and exclusions clearly stated.
13. If shortlisted, participation in a scripted solution demonstration using NCR scenarios and, where requested, a clarification/presentation session.

15. 15. Pricing Requirements

Pricing must be submitted in South African Rand (ZAR), inclusive of VAT unless the bid invitation prescribes otherwise, and must enable NCR to establish the total cost of ownership over the maximum contract period. Hidden or unquoted mandatory costs will not be accepted.

Cost component	Pricing instruction
Annual subscription / licence	State pricing basis (e.g., named users, concurrent users, modules, transactions, records) and all platform/environment charges.
Implementation and configuration	Fixed price, with milestone breakdown including the Month 6 MVP and all subsequent full-scope implementation deliverables.

Data migration	Fixed price by agreed migration scope/wave, including cleansing support, trial migrations and reconciliation.
Integrations	Price each required integration separately, identifying once-off and recurring charges.
Training and skills transfer	Include all agreed training delivery, materials and any certification costs.
Support and maintenance	Annual costs not already included in subscription; state support hours and inclusions. All costs necessary to provide, implement, test, monitor, maintain and evidence mandatory security controls—including security resources, tooling, assurance, penetration testing, vulnerability remediation, logging, incident response, backup/DR and secure exit—must be included and clearly identified. Security required by this Terms of Reference may not be priced as an optional item.
Payment gateway / messaging	Disclose transaction, SMS or other consumption-based third-party charges and who contracts with the third party.
Optional modules/services	Separately identify optional items; optional pricing must not obscure the price of mandatory scope.
Change-request rate card	Hourly/daily rates by role for approved out-of-scope changes and transition assistance.
Escalation	State annual escalation methodology/percentage. Pricing assumptions must remain fixed for the periods specified in the final contract.

16. 16. Evaluation Approach

The final bid will be evaluated in accordance with NCR supply-chain-management requirements and the applicable preference point system. Mandatory compliance will be assessed before functionality. Bidders meeting the functionality threshold will proceed to price and preference evaluation as specified in the bid invitation.

1. 16.1 Functional Evaluation

A minimum functionality threshold of 70% is recommended to proceed to price and preference evaluation. The following consolidated weighting gives additional emphasis to credible delivery of the six-month MVP.

Criterion	Weight	Criterion-specific rating guide (0–5)
Functional fit to the required regulatory lifecycle and integrations	25%	**0:** No response or no relevant capability demonstrated. **1:** Addresses less than half of the required lifecycle; major modules and integrations are absent or dependent on substantial custom development. **2:** Partially addresses the lifecycle; several material functional or integration gaps remain. **3:** Meets most requirements through standard functionality and configuration; gaps are manageable and clearly addressed.

		4: Meets all material lifecycle and integration requirements with strong end-to-end traceability and only minor limitations. **5:** Fully meets or exceeds requirements through proven, integrated standard capability, supported by compelling evidence and demonstration.
Configurability, maintainability and NCR ability to extend the solution without vendor dependence	15%	**0:** No configurability or maintainability approach provided. **1:** Changes are predominantly vendor-coded; NCR has little or no administrative control. **2:** Limited configuration is available, but routine changes remain substantially vendor-dependent. **3:** NCR administrators can maintain agreed fields, forms, roles, templates and reports using supported tools, with some vendor dependence for workflows or complex changes. **4:** Broad configuration capability, sound upgrade support and effective administration tools enable NCR to implement most routine changes independently. **5:** Extensive, proven no-code/low-code administration, strong governance and documentation, and demonstrated NCR self-sufficiency with minimal vendor dependence.
MVP and implementation approach, including credibility of Month 6 delivery and the post-MVP full-scope plan	20%	**0:** No credible implementation plan or no commitment to the Month 6 MVP. **1:** Plan is materially incomplete or unrealistic, with major omissions in resources, dependencies, testing, migration or acceptance. **2:** Month 6 delivery is asserted but weakly supported; significant feasibility, sequencing or resourcing risks remain. **3:** Credible phased plan covers MVP and post-MVP delivery, with adequate resources, dependencies, testing, migration and governance. **4:** Detailed, well-resourced and low-risk plan demonstrates strong traceability to the MVP acceptance gate and clear post-MVP milestones. **5:** Exceptional evidence of rapid comparable delivery, fully integrated planning and robust contingency measures provides high confidence in Month 6 acceptance and full-scope completion.
Relevant solution experience and reference sites	15%	**0:** No relevant experience or verifiable references provided. **1:** Minimal experience, with no materially comparable implementation. **2:** Some relevant solution experience, but references are limited in scale, scope or comparability. **3:** At least three verifiable relevant implementations, including comparable regulatory, oversight, professional or membership environments. **4:** Strong record of successful comparable implementations with positive references and evidence across most required modules. **5:** Extensive, highly comparable and independently verifiable experience, including multiple successful implementations of similar scale, complexity and regulatory scope.

Local support model, service levels and ongoing product maintenance	10%	**0:** No acceptable support or maintenance proposal. **1:** Support model is unclear, lacks accountable local capability or omits critical maintenance obligations. **2:** Basic support is proposed, but service levels, escalation, staffing or maintenance arrangements contain material weaknesses. **3:** Meets the required local support, service desk, escalation, patching, upgrade and reporting expectations. **4:** Strong local support capacity, measurable service levels, proactive monitoring and well-defined maintenance and escalation arrangements. **5:** Highly mature, proven support operation exceeding baseline service levels, with strong resilience, transparency, continuous improvement and reference evidence.
Security, POPIA, data ownership, resilience and exit arrangements	10%	**0:** No adequate response or unacceptable security, privacy or data-ownership risk. **1:** Major control gaps exist in security, POPIA, hosting, backup, recovery, ownership or exit. **2:** Partial controls are described, but assurance evidence or important resilience and exit provisions are weak. **3:** Meets specified security, privacy, data ownership, backup, recovery, portability and exit requirements with adequate evidence. **4:** Strong independently assured controls, clear hosting and sub-processor transparency, tested resilience and a comprehensive exit approach. **5:** Exemplary security and privacy governance, robust independent assurance, demonstrably tested resilience and highly practical data portability and exit safeguards.
Training, adoption and skills transfer	5%	**0:** No training, adoption or skills-transfer proposal. **1:** Proposal is generic and limited to basic end-user training. **2:** Some role-based training is included, but adoption, administrator enablement or competence evidence is inadequate. **3:** Adequate role-based training, train-the-trainer, guides, adoption activities and structured administrator skills transfer are provided. **4:** Comprehensive, practical programme includes reusable materials, competency assessment, administrator enablement and post-go-live reinforcement. **5:** Exceptional and proven adoption and capability-building approach delivers measurable user proficiency and demonstrable NCR administrator independence.
Total	**100%**	**Maximum weighted functionality score: 100 points. Minimum qualifying threshold: 70 points (70%).**

1. 16.1.1 Evaluation Reference and Evidence Matrix

The evaluation committee must use this matrix with the criterion-specific rating guide in Section 16.1. For every score, evaluators must record the exact bidder proposal page, annexure, schedule, reference letter, certificate, demonstration result or clarification relied

upon. A statement of compliance without verifiable supporting evidence must not receive the same score as an evidenced and demonstrable capability. Evidence must relate to the solution, team and delivery approach proposed for NCR.

Evaluation criterion	TOR reference	Required bidder evidence / evaluation source	Evaluator evidence record
Functional fit to the required regulatory lifecycle and integrations — 25%	Sections 2.2; 4; 6.1–6.4; 7.2–7.3; 8 (NFR-03, NFR-04, NFR-09 and NFR-11); 13 (MR1–MR3); 14 items 1–6; 16.2; and 19.	Completed requirement compliance and traceability matrix covering M1–M12, MVP-01–MVP-12 and relevant NFRs; solution architecture and data flows; standard-versus-configuration-versus-extension statement; interface/API specifications; screenshots or product documentation; reference-site confirmation; and scripted demonstration results showing end-to-end NCR scenarios.	Record proposal page(s), matrix row/reference, annexure, demonstrated scenario and evaluator observation. Identify every material gap, dependency, custom extension, roadmap item or exception.
Configurability, maintainability and NCR ability to extend the solution without vendor dependence — 15%	Sections 2.2; 3; 6.2; 6.5; 8 (NFR-15 and NFR-16); 10 (D2, D11 and D13); 12; 13 (MR2 and MR6); 13.1; 14 items 1, 8 and 9; 16.2; and 17.2.	Configuration catalogue; administrator-tool description; list of fields, forms, rules, roles, templates, workflows and reports maintainable by NCR; product upgrade approach; custom-extension register; administration documentation; proposed skills-transfer and competency-assessment plan; sample guides; licensing/access needed for NCR administration; and live demonstration of an authorised administrator making an agreed change without vendor code.	Record proposal page(s), configuration function demonstrated, administration role used, steps completed, limitations, vendor intervention required, upgrade impact and supporting document/reference.
MVP and implementation approach, including credibility of Month 6 delivery and the post-MVP full-scope plan — 20%	Sections 5; 6.3–6.5; 7.1–7.4; 9; 10 (D1–D10); 13 (MR3); 13.1; 14 items 3–6 and 10; 17; and 18.	Signed Month 6 commitment; detailed resource-loaded project plan with critical path and post-MVP milestones; work breakdown structure; named team and availability; mobilisation, design, configuration, integration, migration, testing, security, training, cut-over and acceptance activities; dependencies and RAID register; governance and reporting approach; contingency and recovery plan; and evidence of comparable rapid implementations.	Record proposal page(s), plan or schedule reference, milestone/date, named resource, dependency, risk and mitigation. Note whether each MVP acceptance-gate requirement is traceable to an activity, owner, deliverable and acceptance date.
Relevant solution experience and reference sites — 15%	Sections 13 (MR1 and MR4); 13.1; 14 item 11; 16.1 rating guide; and 19.	At least three signed or independently verifiable client references, including the required comparable environments; client name and contact details; implemented modules, scope, scale, contract period,	Record reference letter or proposal page, client, contact-verification outcome, comparable modules, scale, dates, product, bidder role and any qualification.

		implementation status and go-live date; evidence of the proposed product/version and bidder's role; performance or completion evidence where available; and CVs demonstrating relevant delivery experience.	Do not count duplicate, unverifiable or materially non-comparable references without explanation.
Local support model, service levels and ongoing product maintenance — 10%	Sections 5; 8 (NFR-02, NFR-08, NFR-14 and NFR-15); 10 (D10 and D12); 11.1–11.2; 13 (MR4 and MR5); 13.1; 14 item 8; 15; 17.2; and 18.	South African support presence or binding partner arrangement; service-desk operating model; named support structure and escalation matrix; support hours and 24x7 critical escalation; proposed SLA with response, restoration, availability, RPO/RTO and reporting commitments; monitoring, patching, release and problem-management processes; product roadmap and maintenance policy; sample service report; service credits; and relevant support references.	Record proposal page(s), SLA schedule, committed values, support location, accountable resource/partner, escalation level, included versus chargeable service, evidence of tooling/process maturity and evaluator findings.
Security, POPIA, data ownership, resilience and exit arrangements — 10%	Sections 2.1–2.2; 3; 5; 6.3–6.4; 7.2–7.3; 8 (NFR-01 and NFR-03–NFR-11, NFR-16); 10 (D2, D4, D8, D10, D12 and D13); 11; 12; 13 (MR7); 13.1; 14 item 7; 15; 17.2; and 18.	Proposal-specific security and privacy plan and control matrix; security architecture and data flows; POPIA compliance response; hosting, data-location and sub-processor disclosure; ISO/IEC 27001, SOC 2 Type II or equivalent assurance; recent penetration-test summary and remediation status; identity, privileged-access, encryption/key-management, vulnerability/patching, logging/monitoring, incident-response and breach procedures; backup/DR design and test evidence; committed RPO/RTO; data ownership, export, retention, deletion and secure-exit plans; and confirmation of included security costs.	Record proposal page(s), control/NFR reference, certificate or report details and validity, test date/result, unresolved finding, hosting/sub-processor location, committed RPO/RTO and portability/exit evidence. Clearly identify exceptions, residual risks and missing assurance.
Training, adoption and skills transfer — 5%	Sections 2.2; 3; 6.5; 7.3–7.4; 10 (D9 and D11); 13 (MR6); 13.1; 14 item 9; and 17.	Role-based training needs analysis and plan; curricula for users, managers, ICT and business administrators; train-the-trainer approach; sample manuals, quick guides and recordings; change, communication and adoption plan; training schedule and resource allocation; attendance and completion evidence; competency assessment and administrator certification/accreditation where	Record proposal page(s), course/module, target role, delivery method, duration, trainer qualification, assessment method, completion standard, reusable material, post-go-live support and evidence that NCR administrators will become independently competent.

		available; post-go-live reinforcement; and measurable adoption and skills-transfer outcomes.	

Evaluation evidence rule: Each evaluator must independently record the evidence supporting the raw score before moderation. The moderated record must capture the final score, agreed evidence references, material strengths, gaps, risks, assumptions and reasons for any adjustment. Clarifications may confirm or explain submitted information but must not introduce a materially new solution, team, capability or evidence after bid closure, subject to the applicable NCR SCM rules.

2. *16.2 Scripted Demonstration*

Shortlisted bidders **will** be required to demonstrate the proposed solution using NCR-defined scenarios. At minimum, the demonstration should cover an end-to-end application from public intake to approval/registration, payment/financial status, public verification, and a complaint or investigation that results in an entity status change. NCR may require bidders to show how an authorised administrator changes a form, workflow, status, template or report without vendor code changes.

3. *16.3 Scripted Demonstration Evaluation Criteria*

The scripted demonstration is a separate scored evaluation stage for shortlisted bidders and will be assessed out of 100 points. The bidder must demonstrate the proposed solution and version using NCR-issued scenarios, representative roles and realistic data. Narration, slides, mock-ups, screenshots, videos, prototypes or roadmap commitments will not be accepted as a substitute for demonstrable live capability. The demonstration score must be based only on capability observed and evidence recorded during the session.

Scripted demonstration criterion	Maximum points	Minimum demonstration coverage and evidence	Criterion-specific rating guide (0–5)
1. End-to-end regulatory lifecycle and functional fit	**30**	Demonstrate a complete NCR-defined application journey from public intake, validation and supporting documents through work allocation, assessment, additional-information handling, approval, registration/certificate issue, payment or financial-status exchange, public verification and audit history. Demonstrate a complaint or investigation linked to the same or another entity, including outcome and status impact. Evaluators must verify workflow continuity, entity linkage, notifications, role controls, documents, correspondence and reporting. References: Sections 4, 6.1, 6.3, 7.2 and 8.	**0:** No live demonstration, materially different solution, or core scenario cannot be started. **1:** Less than half the lifecycle is shown; demonstration is mainly narrated, mocked up or fragmented; major modules are absent. **2:** Several lifecycle stages are demonstrated, but material gaps, manual hand-offs, broken entity linkage or substantial custom work remain. **3:** The complete minimum scenario is demonstrated with adequate workflow continuity, controls,

			records and outputs; minor manageable gaps exist. **4:** All material stages are demonstrated smoothly through integrated standard/configured capability, with strong traceability and only minor limitations. **5:** Fully integrated end-to-end capability is demonstrated without material gaps, including strong exception handling, auditability, usability and compelling evidence of operational readiness.
2. Configuration, maintainability and NCR administrator independence	**20**	Using standard supported tools and an authorised administrator role, demonstrate creation or amendment of an agreed field, form rule, workflow step, status, role, template, fee or report; publish the change to an appropriate environment; show versioning, approval and audit history; and explain upgrade impact. The demonstration must distinguish standard functionality, configuration and custom extension. References: Sections 3, 6.2, 6.5, 8 (NFR-15), 12 and 13 (MR2 and MR6).	**0:** No configuration capability is demonstrated. **1:** Changes require vendor coding or technical intervention; NCR administrator control, governance and auditability are not demonstrated. **2:** Limited changes are demonstrated, but publishing, versioning, approval, audit history or upgrade support is incomplete and vendor dependence remains material. **3:** An authorised administrator completes and publishes the minimum agreed change using supported tools, with adequate governance, versioning and audit evidence. **4:** Multiple representative changes are completed efficiently, with strong separation of duties, rollback/version control, documentation and limited vendor dependence. **5:** Extensive no-code/low-code self-sufficiency is demonstrated across

			forms, rules, workflows, roles, templates and reports, with exemplary governance and clear upgrade-safe operation.
3. Integration, data migration and information integrity	**15**	Demonstrate or execute an NCR-issued integration scenario showing secure API exchange, validation, error handling, retry or reconciliation and monitoring. Demonstrate import or migration of representative records, duplicate detection, exception handling, source-to-target reconciliation and preservation of key relationships and documents. Where a live external dependency is unavailable, NCR may permit a controlled test harness, but the bidder must expose actual messages, logs and results. References: Sections 6.3–6.4, 7.2 (MVP-06 and MVP-11), 8 (NFR-09 and NFR-11) and 10 (D6–D8).	**0:** No integration or migration capability is demonstrated. **1:** Demonstration is largely conceptual or mocked; actual messages, logs, controls and reconciliation evidence are absent. **2:** Basic exchange or import works, but material weaknesses exist in security, validation, error handling, duplicate control, relationship preservation or reconciliation. **3:** The minimum API and migration scenarios execute successfully with adequate validation, exception handling, monitoring and source-to-target reconciliation. **4:** Secure bidirectional exchange, recovery/retry, monitoring and robust migration controls are demonstrated with only minor limitations. **5:** Complex integration and migration scenarios are demonstrated end to end with strong automation, security, observability, data integrity, exception recovery and compelling reconciliation evidence.
4. Security, privacy, auditability and resilience	**20**	Demonstrate SSO/MFA or equivalent test identity controls, role-based and privileged access, segregation of duties, protection of confidential records, tamper-evident audit logs, security alerts or monitoring evidence, and secure API or data-transfer controls. Show backup status and recovery evidence, security administration, vulnerability or patch status and incident evidence appropriate to the solution. No	**0:** Security controls are not demonstrated or an unacceptable security/privacy exposure is observed. **1:** Only basic login or generic security claims are shown; major gaps exist in access control, audit, monitoring, resilience or privacy.

		sensitive production data may be used. References: Sections 2.1, 3, 7.3, 8 (NFR-03–NFR-11), 11, 12, 13 (MR7) and 18.	**2:** Some controls operate, but material gaps remain in MFA/privileged access, segregation, confidential records, logging, vulnerability status, backup or recovery evidence. **3:** All minimum controls are adequately demonstrated with current evidence and no unmitigated critical or high-risk issue observed. **4:** Strong integrated controls, monitoring, auditability, secure data exchange and tested recovery are demonstrated with independent assurance and only minor limitations. **5:** Exemplary defence-in-depth, privacy by design, privileged-access governance, tamper-evident audit, active monitoring, incident readiness and demonstrably tested resilience are shown with compelling assurance evidence.
5. Reporting, usability, accessibility and operational readiness	**15**	Demonstrate role-based dashboards and reports, filtering and drill-down, scheduled and ad hoc output, Excel/CSV export, turnaround and backlog visibility, audit or management reporting, mobile-responsive public access and applicable accessibility features. Show support or operational monitoring, user guidance and readiness for real NCR use. References: Sections 6.1 (M9, M11 and M12), 6.5, 8 (NFR-02, NFR-12–NFR-14), 10 (D9–D12) and 11.	**0:** No usable reporting, public-access or operational-readiness capability is demonstrated. **1:** Only static or generic reports are shown; usability, accessibility and operational readiness are materially deficient. **2:** Basic dashboards or reports work, but material gaps exist in drill-down, scheduling, export, turnaround/backlog visibility, mobile access, accessibility or support readiness. **3:** The minimum reporting, export, public-access, usability and

			operational-readiness requirements are adequately demonstrated. **4:** Strong role-based analytics, flexible reporting, responsive and accessible user journeys, monitoring and user-support features are demonstrated with minor limitations. **5:** Exceptional, intuitive and accessible operational capability is demonstrated, including advanced yet usable analytics, effective drill-down, automation, reliable outputs and compelling readiness for real NCR use.
Total	**100**	**Maximum scripted demonstration score: 100 points.**	**Evaluators must select one whole-number rating from 0 to 5 for each criterion and convert it using the formula below the table.**

Scoring methodology: For each criterion, evaluators will award a raw rating from 0 to 5 and convert it to points using: awarded points = (raw rating ÷ 5) × criterion maximum points. Rating 0 = not demonstrated; 1 = materially deficient or mostly narrated; 2 = partially demonstrated with material gaps; 3 = adequately demonstrated and meets the minimum requirement; 4 = strongly demonstrated with minor limitations; 5 = fully demonstrated, integrated and supported by compelling verifiable evidence. Scores must reflect what was demonstrated, not unverified claims in the written proposal.

Minimum qualifying requirements: A bidder must achieve at least 70 points out of 100 overall. Failure to demonstrate a mandatory capability, use of a materially different product or version from that proposed, or reliance on undisclosed future roadmap functionality may result in a score of zero for the affected criterion and may be treated in accordance with the bid conditions and NCR SCM rules.

Demonstration governance and evidence: NCR will issue the final script, order of scenarios, time allocation and test data uniformly to shortlisted bidders. The bidder's proposed key personnel must conduct the demonstration.

17. 17. NCR and Service Provider Responsibilities

1. 17.1 NCR Responsibilities

- Provide timely access to nominated business and ICT subject-matter experts, decision-makers and project governance forums.
- Provide agreed source data, legacy-system extracts, interface specifications/credentials and access to NCR-controlled environments or third-party services where required.
- Review and approve deliverables, decisions and test outcomes within agreed governance timelines.
- Nominate users for testing, training and skills transfer.
- Approve production go-live after satisfaction of the applicable acceptance gate.

2. 17.2 Service Provider Responsibilities

- Manage and deliver the complete contracted solution and remain accountable for all subcontractors and platform dependencies.
- Proactively identify dependencies, risks and decisions that could affect the Month 6 MVP or approved post-MVP full-scope milestones and escalate them early with mitigation actions.
- Provide appropriately skilled resources and maintain continuity of key personnel; replacements must have equivalent or better capability and require NCR approval where specified in the contract.
- Protect NCR information and comply with agreed security, privacy, audit, records and operational requirements.
- Provide, implement and maintain the security measures committed in the accepted proposal and approved security and privacy plan; supply evidence of control operation; continuously monitor threats and vulnerabilities; promptly report and contain incidents; remediate weaknesses within agreed timeframes; and ensure equivalent controls apply to all personnel, platform vendors, subcontractors and sub-processors.
- Produce complete documentation sufficient for NCR to operate, administer, audit and transition the service.

3. 17.3 Joint Ventures, Subcontractors and Third-Party Involvement

Mandatory proposal disclosure and evidence: The bidder must disclose every joint-venture member, consortium member, subcontractor, implementation partner, platform or hosting provider, sub-processor and other third party that will perform, support or enable any part of the contract. The proposal must provide, for each party, its full legal name, registration and tax/CSD details where applicable, ownership and B-BBEE information where required, physical and data-processing locations, exact scope and percentage/value of work, deliverables, resources and key personnel, access to NCR information or systems, security and POPIA role, service dependencies, fees and recurring charges, and the proposed governance and escalation arrangements.

The bidder must submit signed joint-venture, consortium, partnership or subcontracting agreements, letters of commitment, authority of the lead member, allocation of responsibilities, relevant licences or vendor authorisations, due-diligence evidence, conflict-of-interest declarations and proof that each proposed party has the capacity and right to perform its allocated work. A bidder may not rely on an unnamed, uncommitted or undisclosed party to satisfy a mandatory requirement, experience requirement, local-support obligation or evaluation criterion.

Prior approval and change control: No subcontracting, delegation, novation, substitution, addition, removal or material change in the role, ownership, control, work allocation, key personnel, hosting location, sub-processing arrangement or dependency of any disclosed party may occur after bid closure or during the contract without NCR's prior written approval and completion of NCR-required due diligence and change control. NCR may reject a proposed party or change where it creates legal, procurement, B-BBEE, conflict-of-interest, capacity, security, privacy, financial, operational, reputational or continuity risk. Approval does not create a contractual relationship between NCR and that party, does not release any joint-venture member or the appointed service provider from its obligations, and does not entitle the service provider to additional cost, time or scope relief unless NCR expressly approves it through formal change control.

Accountability and flow-down obligations: The appointed service provider and, where applicable, all joint-venture members will remain jointly and severally responsible for full, timely and compliant performance. The service provider remains the single accountable point of contact and is liable for every act, omission, delay, breach, control failure and service-level failure of its joint-venture members, subcontractors and third parties as if it were its own. It must impose written obligations that are no less stringent than the NCR contract, including confidentiality, POPIA and information-security controls, personnel screening, intellectual-property and data ownership, records retention, audit access, incident notification, business continuity, service levels, anti-fraud and conflict-of-interest controls,

ethical conduct, legal and regulatory compliance, insurance, cooperation with investigations, exit assistance, data return and verified secure deletion. NCR may inspect and audit relevant records, controls, premises and performance directly or through an authorised assurance provider, subject to appropriate confidentiality safeguards.

Ongoing management, continuity and remedies: The service provider must maintain an up-to-date register of all approved parties and sub-processors, monitor their capacity, performance, security, compliance and financial or operational risk, and report material changes, incidents and failures to NCR immediately. It must maintain effective contingency, step-in, substitution and orderly-exit arrangements so that the failure, insolvency, withdrawal or replacement of any party does not interrupt NCR services or compromise NCR information. Undisclosed or unauthorised third-party involvement, misrepresentation of work allocation or capabilities, failure to flow down mandatory obligations, or failure to remedy a third-party breach may be treated as a material breach and may result in rejection or disqualification where applicable, withholding of acceptance or payment, required replacement at the service provider's cost, enforcement of contractual remedies, damages, suspension or termination, subject to the bid conditions, signed contract and applicable NCR SCM requirements.

18. 18. Risk Identification and Mitigation: Service Provider and NCR

Risk management will be a joint and continuous responsibility throughout mobilisation, implementation, go-live, support and contract exit. The service provider must maintain a current risk and dependency register, assign accountable owners, assess likelihood and impact, implement agreed controls, report residual exposure and escalate material risks through the project governance structure. NCR will manage the risks and dependencies within its control and will provide timely decisions, access and oversight.

Neither party is relieved of its contractual obligations by identifying a risk, and any change to scope, cost or milestones remains subject to formal NCR-approved change control.

Risk owner	Risk identification	Potential impact	Required mitigation and control
Service provider	Insufficient mobilisation, specialist capacity, key-person dependency or unapproved replacement of critical resources.	Delayed MVP or full-scope delivery, reduced quality and knowledge gaps.	Submit and maintain a resource-loaded plan; secure named key personnel and backups; monitor capacity weekly; obtain NCR approval for specified replacements; and implement recovery plans at the service provider's cost where delay is supplier-attributable.
Service provider	Proposed product, configuration or integration capability does not meet mandatory requirements or relies on immature roadmap functionality.	Functional gaps, excessive customisation, upgrade constraints and failure of acceptance.	Complete traceability to proven standard capability; demonstrate material functions before award; disclose all gaps and custom extensions; prototype high-risk integrations early; and apply contractual acceptance criteria and remedies.
Service provider	Inadequate planning, testing, defect management, quality assurance or release control.	Production defects, disrupted operations, rework and missed milestones.	Maintain approved test and quality plans; use entry and exit criteria for each test stage; retain complete evidence; resolve Severity 1 and 2 defects before go-

			live; conduct release-readiness reviews; and maintain tested rollback procedures.
Service provider	Data migration errors, incomplete records, duplicate entities or failed reconciliation.	Loss of data integrity, inaccurate regulatory decisions and operational disruption.	Perform profiling, mapping, cleansing support, trial migrations and exception management; reconcile to NCR-approved control totals; retain source-to-target audit evidence; secure NCR sign-off; and maintain tested rollback and restoration arrangements.
Service provider	Cybersecurity incident, privacy breach, unauthorised access, vulnerable subcontractor or hosting failure.	Compromise of personal or regulatory information, service interruption, legal exposure and reputational damage.	Apply security and privacy by design; enforce MFA, least privilege, encryption, logging and vulnerability management; disclose and control sub-processors; maintain incident response and breach-notification procedures; conduct independent assurance and penetration testing; and remediate findings within agreed periods.
Service provider	SaaS outage, inadequate backup or disaster-recovery capability, or failure to meet service levels.	Unavailable regulatory services, transaction backlogs and loss of stakeholder confidence.	Meet contracted availability, RPO and RTO commitments; monitor service health; maintain resilient hosting and verified backups; test disaster recovery at least annually; report incidents and root causes; and apply service credits and corrective-action plans for failures.
Service provider	Uncontrolled subcontractor, platform-vendor or third-party dependency, including payment, messaging and integration services.	Delivery delays, increased costs, control gaps or service interruption.	Remain fully accountable for third parties; disclose dependencies, contracts, locations and charges; perform due diligence; maintain enforceable service and security obligations; provide continuity and substitution plans; and escalate dependency risks early.
Service provider	Vendor lock-in, inadequate documentation, poor skills transfer or ineffective exit support.	Operational dependence, increased lifecycle cost and difficulty transitioning the service.	Provide current technical and operational documentation; deliver competency-based skills transfer; enable routine NCR administration; support periodic data exports in usable non-proprietary formats; maintain an exit plan; and complete knowledge transfer, data handover and deletion certification.
NCR	Delayed decisions, approvals, access, governance escalation or availability of subject-matter experts.	Blocked activities, schedule slippage and avoidable supplier standby.	Confirm governance roles and delegated authority at mobilisation; nominate accountable business and ICT leads; maintain decision and action logs; apply agreed review timeframes; provide escalation routes; and promptly communicate constraints.

NCR	Incomplete, poor-quality or late source data and undocumented legacy rules.	Migration delays, reconciliation exceptions and inaccurate configuration.	Identify authoritative data owners; provide extracts to agreed dates and formats; approve cleansing and mapping rules; validate control totals; resolve exceptions; and formally sign off migrated data.
NCR	Limited user participation in requirements validation, testing, training or change adoption.	Unfit configuration, delayed acceptance, low adoption and continued manual workarounds.	Secure business ownership and user availability; approve representative scenarios; enforce UAT participation and sign-off; implement communications and readiness plans; monitor training completion and adoption; and address resistance through accountable managers.
NCR	Delayed provision of interface specifications, credentials, environments or third-party approvals controlled by NCR.	Late integration testing and risk to the Month 6 MVP.	Confirm interface owners and prerequisites at mobilisation; establish access lead times; track dependencies in the integrated plan; provide test facilities and credentials securely; and escalate delays through governance.
NCR	Scope growth, conflicting stakeholder requirements or informal change requests.	Cost escalation, rework, diluted MVP focus and delayed delivery.	Maintain an approved baseline and prioritised backlog; appoint authorised decision-makers; require documented impact assessments; reject informal changes; and approve changes only through formal scope, budget and schedule control.
NCR	Insufficient budget provision, delayed payment or unavailable funding for approved lifecycle costs.	Interrupted delivery, reduced support coverage or inability to use required services.	Validate total cost of ownership before award; align milestones with approved budgets and accepted deliverables; monitor commitments and consumption charges; process valid invoices within agreed terms; and plan contract extensions and escalations in advance.
Joint	Failure to identify, assess, escalate and treat emerging project, operational, security, compliance or continuity risks.	Unmanaged residual exposure, governance failure and avoidable service disruption.	Maintain a single RAID register with owners, due dates, likelihood, impact, controls and residual ratings; review it weekly during implementation and monthly during support; escalate high and critical risks promptly; record accepted risks and approvals; and track mitigation to verified closure.

19. 19. General Conditions and Clarifications

- Any conflict between a bidder's standard terms and the final NCR contract will be resolved in favour of the signed contract and bid conditions.
- All bidder assumptions, exclusions, third-party dependencies, data-volume limits, usage thresholds and additional charges must be stated explicitly in the bid response.

- Roadmap functionality will not be treated as meeting a mandatory MVP requirement. For non-MVP requirements, any roadmap commitment must include a firm release date and contractual remedy if not delivered.
- The NCR reserves the right to validate reference information, request clarifications, conduct due diligence and require demonstration of claimed product capability before award.
- Project meetings may be held at NCR offices and/or through Microsoft Teams. Any chargeable travel must be separately identified in the pricing response.

End of the Tender document