REQUEST FOR INFORMATION (RFI)

RFI001-2026: REQUEST FOR INFORMATION FOR MAINTENANCE, SUPPORT, ENHANCE AND FURTHER DEVELOPMENT OF THE EXISTING NATIONAL TREASURY SAFETYWEB BANKING SYSTEM FOR A PERIOD OF THREE (3) YEARS

CLOSING DATE AND TIME OF RFI

04 SEPTEMBER 2026 AT 11H00

national treasury

Department:
National Treasury
REPUBLIC OF SOUTH AFRICA

A NATION THAT WORKS

1. INTRODUCTION

1.1 The National Treasury (NT), through the Office of the Accountant-General (OAG), invites suitably qualified service providers to submit Request for Information (RFI) for the maintenance, support, enhancement and further development of the existing National Treasury-owned SafetyWeb Banking System for a period of three (3) years.

1.2 The SafetyWeb Banking System is a critical banking, payment validation and fraud prevention application that supports the banking services provided by the OAG. The system is utilised by NT Pay Master General (PMG) users and authorised users from National Departments and other participating government entities. It supports payment processing and banking operations while performing critical validation, verification and fraud prevention controls to help ensure that only authorised, accurate and legitimate payment transactions are processed, thereby reducing the risk of duplicate, invalid, unauthorised and fraudulent payments.

2. BACKGROUND

2.1 The Office of the Accountant-General (OAG) has a mandate to render banking services to national departments.

2.2 The National Treasury (NT) has full ownership of the SafetyWeb Banking System, which is used by the Office of the Accountant-General (OAG) to provide banking services to National Departments and authorised government entities. The future Service provider will be appointed solely to provide maintenance, support, enhancement and further development services for the existing system and will not acquire any ownership rights, intellectual property rights or proprietary interests in the SafetyWeb Banking System.

2.2.1 The SafetyWeb Banking System processes transactions with a value exceeding approximately R400 billion per month. The system provides critical preventative and detective controls designed to identify duplicate, invalid, unauthorised and potentially fraudulent payment transactions before payment is released. The continued availability, integrity and security of the system are therefore essential to safeguarding public funds and maintaining confidence in government payment processes.

2.2.2 The Service provider shall provide support during NT business hours on every working day, including the period between Christmas and New Year when the NT is officially closed but the Office of the Accountant-General remains operational. Service provider should indicate their proposed after-hours, weekend and public holiday support arrangements for Priority 1 incidents.

Priority	Description
1	As soon as possible- if possible other tasks are to be suspended in order to implement this task. Change to commence immediately. These will mostly relate to processing of daily payments, submitting of account verification files and creating of daily bank statement to all the respective account holders.

	Should be corrected within a maximum of 8 hours since logging the request.
2	High- change to commence once any other task has been completed.
3	Medium-. Change to be scheduled to start when staff is available (or at some specific point in the future)
4	Low- change to be done when convenient.

2.3 The service provider should provide support for Connect, web service, and server-related issues, including collaborating with NTICT on the setup and configuration of new servers, conducting vulnerability assessments, and performing other related server support activities as required.

3. CURRENT SAFETYWEB ENVIRONMENT

3.1 The SafetyWeb Banking system is a webenabled system and is used for the following:

3.1.1 Validation and fraud prevention controls to detect and prevent duplicate, invalid, unauthorised or potentially fraudulent payment transactions prior to processing;

3.1.2 Daily local and foreign payments in ISO 20022 layout;

3.1.3 Electronic verification of banking details of suppliers/beneficiaries including Central Supplier Database, SASSA and Government Pension Fund;

3.1.4 Daily electronic fund payments (EFT's) report submitted to CFO's identifying payments to unverified supplier bank accounts;

3.1.5 Daily Cash Management report used by Asset and Liability Management Division;

3.1.6 Daily electronic bank statements to all National departments and other entities that operate within the PMG banking system. At least 83 bank accounts in total including SASSA, Penions, Water Trading and Public Works Trading;

3.1.7 The system monitors all grant payments made by the respective departments for the amount and date against the approved payment schedule. If the payment does not meet the requirements of the payment schedule should be rejected;

3.1.8 Monthly request for funds (RFF) against approved monthly drawing schedule; and

3.1.9 Monthly automated RFF report to budget office.

4. CURRENT TECHNICAL ENVIRONMENT

4.1 The SafetyWeb Banking System is a critical application that supports the banking services provided by the Office of the Accountant-General. The system operates within the NTICT environment and interfaces with various internal and external systems to facilitate secure banking operations and payment processing.

4.2 The current technical environment includes, but is not limited to the following:

4.2.1 Application environment:

4.2.1.1 A web-enabled application architecture hosted within the NT infrastructure;

4.2.1.2 Operating System: Microsoft Windows Server 2025 Standard;

4.2.1.3 Web Server: Microsoft Internet Information Services (IIS); and

4.2.1.4 Application Framework: Microsoft .NET Framework 4.8.1

4.2.2 Database Environment:

4.2.2.1 Database Platform: Microsoft SQL Server 2022

4.2.2.2 Operating System: Microsoft Windows Server 2025 Standard

4.2.3 Integration Environment:

4.2.3.1 The system interfaces with various internal and external systems and stakeholders, including:

4.2.3.1.1. Connect for the secure transfer of files between the NT and external stakeholders;

4.2.3.1.2. Web services supporting system-to-system integration with internal and external applications;

4.2.3.1.3. External interfaces with the South African Reserve Bank (SARB), commercial banks, the Central Supplier Database (CSD), the South African Social Security Agency (SASSA), the Government Employees Pension Fund (GEPF), and other government financial systems, where applicable;

4.2.4 Database administration:

4.2.4.1 Including performance tuning, data integrity, backup and recovery, capacity planning, and database maintenance;

4.2.5 Infrastructure Management

4.2.5.1 Server administration undertaken in collaboration with the NT Information and Communication Technology (NTICT) environment, including server configuration, vulnerability remediation, performance monitoring, and infrastructure upgrades;

4.2.6 Change and Release Management:

4.2.6.1 Change and release management processes to support the implementation of system enhancements, upgrades, security patches, and production releases; and

4.2.7 Environment Management:

4.2.7.1 Production, test, and disaster recovery environments supporting the development, testing, and operation of the SafetyWeb Banking System.

4.3 The Service provider will be expected to work closely with NTICT in supporting the technical environment, including server provisioning, configuration, vulnerability remediation, performance monitoring, infrastructure upgrades, and other related technical activities.

4.4 Service provider are requested to describe their experience in supporting similar technical environments and provide recommendations on industry best practices, technologies, support models, and innovations that could improve the resilience, security, availability, and performance of the SafetyWeb Banking System.

4.5 The technical environment described above reflects the NT's current operating environment and is provided to assist service provider in understanding the existing technology landscape. Service provider should note that the technical environment may evolve during the term of any future contract as a result of technology refreshes, infrastructure upgrades, security requirements, or changes to business needs. The NT therefore seeks information from service provider on their capability to support both the current environment and future technology changes.

5. OBJECTIVES

5.1 The objective of this Request for Information (RFI) is to obtain information from the market regarding the capability, experience, service delivery models, and innovative solutions available for the maintenance, support, enhancement, and further development of the existing NT-owned SafetyWeb Banking System.

5.2 This RFI is issued solely for information-gathering purposes and does not constitute a commitment by the NT to procure any services or award any contract. The information received will assist the NT in determining the most appropriate procurement approach and developing comprehensive technical specifications/Terms of reference for a future procurement process.

5.3 The NT seeks information from the market to ensure that the future solution will:

5.3.1 Ensure the continuous availability, reliability, and stability of the SafetyWeb Banking System in support of the banking services provided by the OAG;

5.3.2 Ensure that the fraud detection, payment validation and preventative control capabilities of the SafetyWeb Banking System remain effective and continue to evolve in response to emerging fraud threats;

5.3.3 Maintain the integrity, confidentiality, and security of banking data and transactions processed through the SafetyWeb Banking System;

5.3.4 Provide timely maintenance, technical support, and problem resolution to minimise disruption to critical banking services;

5.3.5 Support the ongoing enhancement, maintenance, and development of the SafetyWeb Banking System to meet evolving business, legislative, regulatory, and operational requirements;

5.3.6 Ensure the effective management of system upgrades, enhancements, releases, and infrastructure changes while minimising operational risk;

5.3.7 Support and maintain all interfaces between the SafetyWeb Banking System and internal and external stakeholders, including banking institutions and other government systems;

5.3.8 Promote sound project management, governance, risk management, and change management practices throughout the lifecycle of the system;

5.3.9 Ensure that the system continues to support efficient, secure, and accurate payment processing and banking operations for National Departments;

5.3.10 Obtain information on industry best practices, emerging technologies, innovative service delivery models, and opportunities to improve the performance, resilience, security, and sustainability of the SafetyWeb Banking System; and

5.3.11 Identify an appropriate support and resource model that will ensure the continued delivery of a secure, efficient, and responsive banking service to the NT and its stakeholders.

6. SCOPE OF INFORMATION REQUESTED

6.1 The NT intends to appoint a suitably qualified and experienced service provider to provide comprehensive maintenance, support, enhancement and further development services for the existing NT-owned SafetyWeb Banking System.

6.2 The purpose of this RFI is to obtain information from the market regarding the capability, experience and proposed service delivery models for the following services:

6.3 Application Maintenance and Support:

6.3.1 The service provider will be expected to provide ongoing corrective, preventative, adaptive and perfective maintenance to ensure the continuous availability, reliability and optimal performance of the SafetyWeb Banking System.

6.3.2 The services should include defect resolution, system support, performance improvements, technical assistance and the resolution of operational issues affecting the system.

6.4 System Enhancements and Development

6.4.1 The service provider will be expected to undertake system enhancements, new developments, functional improvements and modifications to meet changing business, legislative and operational requirements.

6.4.2 Enhancements may include system improvements, new functionality, data conversions, reporting requirements, integration changes and other improvements identified by the NT.

6.4.3 The service provider shall be expected to apply a structured Software Development Lifecycle (SDLC) for all maintenance, enhancements, upgrades and new developments undertaken on the SafetyWeb Banking System which shall include but not be limited to:

6.4.3.1 Requirements analysis and solution design;

6.4.3.2 Technical design documentation;

6.4.3.3 Secure software development practices;

6.4.3.4 Source code management and version control;

6.4.3.5 Peer code reviews;

6.4.3.6 Unit testing;

6.4.3.7 System testing;

6.4.3.8 Integration testing;

6.4.3.9 Performance testing where applicable;

6.4.3.10 Security testing and vulnerability remediation;

6.4.3.11 User Acceptance Testing (UAT) support;

6.4.3.12 Controlled production deployment;

6.4.3.13 Post-implementation verification; and

6.4.3.14 Maintenance of complete development and release documentation.

6.5 Technical Infrastructure Support

6.5.1 The service provider will be expected to provide technical support relating to the SafetyWeb technical environment, including application servers, web services, Connect, system integrations and related infrastructure in collaboration with NTICT.

6.6 Database Administration

6.6.1 The service provider will be expected to provide database administration services, including database maintenance, performance tuning, backup and recovery, data integrity management, capacity planning and database optimization.

6.7 Systems Integration

6.7.1 The service provider will be expected to maintain and support interfaces between the SafetyWeb Banking System and internal and external systems, including the South African Reserve Bank, commercial banks, the Central Supplier Database (CSD), the South African Social Security Agency (SASSA), the Government Employees Pension Fund (GEPF), and other government financial systems, where applicable.

6.8 Incident, Problem and Change Management

6.8.1 The service provider will be expected to implement and manage effective incident, problem and change management processes, including call logging, issue tracking, root cause analysis, change control, release management and reporting.

6.8.2 The Service provider shall manage all software releases and production deployments using controlled release management processes. This shall include:

6.8.2.1 Release planning;

6.8.2.2 Release documentation;

6.8.2.3 Change approval;

6.8.2.4 Deployment planning;

6.8.2.5 Rollback procedures;

6.8.2.6 Production verification;

6.8.2.7 Release reporting; and

6.8.2.8 Post-implementation reviews

6.9 Service Management and Call Logging System

6.9.1 The service provider shall provide and maintain a call logging and service management system for the management of all incidents, service requests, defects, problems, changes and enhancements relating to the SafetyWeb Banking System.

6.9.2 The call logging system shall provide a central point for the logging, allocation, monitoring, escalation and reporting of all support-related activities and shall enable effective management of service delivery in accordance with agreed service levels.

6.9.3 The service provider shall ensure that the call logging system is available for use by the NT and relevant stakeholders for the duration of the contract.

6.9.4 The call logging system should provide at a minimum, but not be limited to, the following functionality:

6.9.4.1 Logging and tracking of all incidents, service requests, problems, changes and enhancements;

6.9.4.2 Assignment of logged items to appropriate technical resources;

6.9.4.3 Monitoring of response and resolution times against agreed service levels;

6.9.4.4 Escalation of unresolved issues;

6.9.4.5 Communication and progress and status updates to relevant stakeholders;

6.9.4.6 Maintenance of historical records and audit trails;

6.9.4.7 Reporting on incidents, trends, recurring problems and service performance; and

6.9.4.8 Provision of management reports to support governance and service review meetings.

6.10 Operational Support

6.10.1 The service provider will be expected to provide operational support to ensure the continued delivery of banking services, including user support, production support, implementation support and technical assistance to the NT and participating departments.

6.11 Testing Services

6.11.1.1 The service provider shall establish and maintain appropriate testing processes to ensure that all software changes are adequately tested before deployment into production which shall include, where applicable:

6.11.1.1.1. Unit testing;

6.11.1.1.2. System testing;

6.11.1.1.3. Integration testing;

6.11.1.1.4. Regression testing;

6.11.1.1.5. User Acceptance Testing (UAT) support;

6.11.1.1.6. Performance testing;

6.11.1.1.7. Security testing; and

6.11.1.1.8. Production verification testing

6.11.2 UAT testing and sign off

6.11.2.1 The service provider shall support User Acceptance Testing (UAT) by providing test plans, test scripts, defect resolution and implementation support; and

6.11.2.2 No enhancement, upgrade or software release shall be implemented into the production environment without documented approval and sign-off from the NT's authorised business and technical representatives in accordance with approved change management procedures.

6.12 Security and Risk Management

6.12.1 The service provider will be expected to support the security of the SafetyWeb Banking System through vulnerability management, security patching, secure configuration, risk identification and remediation, and assistance during security audits and compliance activities.

6.13 Project Management

6.13.1 The service provider will be expected to provide project management services to coordinate maintenance activities, enhancements, upgrades, new developments and technical resources, while ensuring effective stakeholder engagement, governance, reporting and risk management.

6.14 Knowledge Transfer and Documentation

6.14.1 The service provider will be expected to maintain comprehensive technical and user documentation and provide knowledge transfer to NT personnel to ensure the sustainability of the SafetyWeb Banking System

6.14.2 Source Code Management

6.14.2.1 The service provider shall maintain all source code, scripts, configuration files and related software artefacts in a secure version control repository throughout the contract period.

6.14.2.2 The NT shall retain full ownership of all source code, documentation, configuration, intellectual property and related artefacts developed or modified under the contract.

6.14.2.3 The service provider shall provide the NT with unrestricted access to the source code repository and shall ensure that all source code is handed over at any time upon request and upon contract termination.

6.14.2.4 The SafetyWeb Banking System remains the sole property of the National Treasury. The Service provider shall only be granted access to the system, source code, documentation and related technical artefacts for the purpose of delivering the contracted maintenance, support, enhancement and development services. Such access shall not transfer any ownership, intellectual property rights or commercial rights to the Service provider.

6.15 Industry Best Practices and Innovation

6.15.1 Respondents are requested to provide information on industry best practices, emerging technologies, innovative service delivery models, and recommendations that could enhance the resilience, security, performance, maintainability, and long-term sustainability of the SafetyWeb Banking System. Responses should include, where applicable, information on the following:

6.15.1.1 Cloud readiness and strategies to support future cloud adoption or hybrid deployment models;

6.15.1.2 Automation of operational, administrative, deployment, and maintenance activities to improve efficiency and reduce operational risk;

6.15.1.3 Monitoring, application performance monitoring (APM), infrastructure monitoring, and proactive alerting capabilities;

6.15.1.4 Observability practices, including the use of metrics, logs, traces, dashboards, and analytics to improve system visibility and incident diagnosis; and

6.15.1.5 Zero Trust security principles, including identity and access management, least-privilege access, authentication, authorisation, and continuous security verification.

6.15.1.6 Adaptability to potential changes to technology standards, architecture, integration patterns, data exchange requirements and interoperability needs.

6.16 Business Continuity and Disaster Recovery

6.16.1 The service provider will be expected to support business continuity and disaster recovery activities, including disaster recovery testing, recovery planning and the maintenance of recovery procedures to ensure the continued availability of the SafetyWeb Banking System

6.17 The NT invites service providers to comment on the proposed scope of services and to recommend any additional services, industry best practices or innovative approaches that should be considered in the development of the future Request for Proposal (RFP).

7. INFORMATION REQUIRED FROM SERVICE PROVIDERS

7.1 Service providers are requested to provide information in sufficient detail to enable the NT to assess their capability, experience, proposed service delivery approach, and recommendations regarding the maintenance, support, enhancement and further development of the SafetyWeb Banking System.

7.2 Company Information - service provider should provide:

7.2.1 Company profile;

7.2.2 Number of years in operation;

7.2.3 Office locations;

7.2.4 Details of relevant experience in providing similar services; and

7.3 Relevant experience - service provider should include details of at least three comparable projects undertaken during the past five years AND provide details of their experience in:

7.3.1 Supporting mission-critical banking or financial systems;

7.3.2 Supporting public sector financial management systems;

7.3.3 Supporting Microsoft-based application environments;

7.3.4 Supporting Microsoft SQL Server databases;

7.3.5 Supporting web-enabled applications;

7.3.6 Supporting Connect Direct environments;

7.3.7 Managing interfaces with banking institutions and government systems;

7.3.8 Providing application maintenance, enhancements and production support; and

7.3.9 Supporting payment validation, fraud detection or fraud prevention systems within banking or government payment environments.

7.4 Technical Capability - service provider should describe their capability to provide:

7.4.1 Application maintenance and support;

7.4.2 System enhancements and further development;

7.4.3 Database administration;

7.4.4 Server administration;

7.4.5 Performance monitoring and tuning;

7.4.6 Capacity planning;

7.4.7 Backup and recovery;

7.4.8 Vulnerability remediation;

7.4.9 Web services support;

7.4.10 Connect Direct support;

7.4.11 Disaster recovery support;

7.4.12 Production support; and

7.4.13 Maintain, support and enhance the SafetyWeb Banking System's payment validation, transaction verification and fraud prevention controls to ensure the continued integrity, security and accuracy of payment processing.

7.5 Service Delivery Model - service provider should describe their proposed approach to:

7.5.1 Incident Management;

7.5.2 Problem Management;

7.5.3 Change Management;

7.5.4 Release Management;

7.5.5 Configuration Management;

7.5.6 Call logging and Help Desk services;

7.5.7 Escalation procedures;

7.5.8 Service continuity; and

7.5.9 Knowledge transfer.

7.6 Service Levels

7.6.1 The SafetyWeb Banking System is a critical application supporting government banking services. Service providers are requested to recommend an appropriate Service Level Agreement (SLA) framework for the support and maintenance of the system.

7.6.2 The response should include, but not be limited to, the following:

7.6.2.1 Proposed support hours and availability;

7.6.2.2 Incident priority classifications;

7.6.2.3 Response times for each priority level;

7.6.2.4 Resolution times for each priority level;

7.6.2.5 Escalation procedures for unresolved incidents;

7.6.2.6 System availability targets;

7.6.2.7 Planned maintenance windows;

7.6.2.8 Service performance monitoring and reporting;

7.6.2.9 Recommended key performance indicators (KPIs) for measuring service delivery; and

7.6.2.10 Any additional service level measures considered appropriate for a mission-critical government banking system.

7.7 Project Management - Service provider should describe:

7.7.1 Their proposed project management methodology;

7.7.2 How technical resources would be managed;

7.7.3 How upgrades, enhancements and maintenance activities would be coordinated;

7.7.4 How project risks would be identified and managed; and

7.7.5 The approach to stakeholder communication and reporting.

7.8 Resource Requirements - Service providers are requested to describe the proposed resource model for the delivery of the services and demonstrate that they have the capacity, skills and experience to provide comprehensive support for the SafetyWeb Banking System throughout the contract period.

7.8.1 Service provider should also indicate how they will ensure the retention of critical knowledge and minimise the impact of staff turnover on the continuity and quality of the services provided.

7.8.2 Service provider should provide information on:

7.8.2.1 The proposed organisational structure and governance model for delivering the services;

7.8.2.2 The key resources that will be assigned to the contract, including their roles, responsibilities, qualifications and relevant experience;

7.8.2.3 The proposed Project Manager who will be responsible for the overall management, coordination and performance of the contract;

7.8.2.4 The technical resources that will be responsible for application support, software development, database administration, infrastructure support, systems integration, testing, implementation and project management;

7.8.2.5 The approach to resource planning, succession planning and knowledge transfer to ensure continuity of service throughout the contract period;

7.8.2.6 The arrangements for providing suitably skilled replacement personnel where required, without disruption to the services;

7.8.2.7 The availability of resources to provide support during normal working hours and during periods of increased operational demand, including the period between Christmas and New Year when the Office of the Accountant-General continues to operate;

7.8.2.8 Confirmation that all resources assigned to the contract will be available for security vetting, where required by the NT or any other authorised government authority, and that the Service provider will cooperate fully with such vetting processes; and

7.8.2.9 Confirmation that the Service provider has the necessary capacity to provide all required resources as part of the fixed monthly fee.

7.9 Reporting and Governance - Service provider should describe their proposed reporting and governance framework for the management, support, maintenance, enhancement, testing, release and continuous improvement of the SafetyWeb Banking System throughout the contract lifecycle.

7.9.1 The proposed reporting framework should provide the NT with appropriate visibility of service performance, operational activities, development activities, system improvements, risks, compliance, quality assurance and the overall health and sustainability of the SafetyWeb Banking System.

7.9.2 Service provider should describe the reports, governance structures, review forums and performance measures that will be provided and managed as part of the service delivery model. The response should include, but not be limited to, the following:

7.9.3 Operational reporting - Service provider should describe the proposed operational reporting approach, including:

7.9.3.1 Daily, weekly and monthly operational reporting requirements;

7.9.3.2 Incident, service request and problem management reporting;

7.9.3.3 System availability, performance and capacity monitoring;

7.9.3.4 Production support activities and operational issues;

7.9.3.5 Status of outstanding operational activities;

7.9.3.6 Recurring issues and root cause analysis;

7.9.3.7 Operational trends and improvement recommendations; and

7.9.3.8 Any other operational information required to support effective service management.

7.9.4 Service Level Agreement (SLA) reporting - Service provider should describe the proposed SLA reporting framework, including;

7.9.4.1 Service availability reporting

7.9.4.2 Incident response and resolution performance;

7.9.4.3 Compliance against agreed service levels;

7.9.4.4 Priority-based incident reporting;

7.9.4.5 Escalated incidents and unresolved matters;

7.9.4.6 Service level breaches and corrective actions;

7.9.4.7 Key Performance Indicators (KPIs); and

7.9.4.8 Service improvement actions arising from SLA performance reviews.

7.9.5 Development, Enhancement and Maintenance Reporting - Service provider should describe the reporting that will be provided for application maintenance, enhancements, upgrades and further development activities, including:

7.9.5.1 Development progress and status of approved work items;

7.9.5.2 Enhancement requests and change requests;

7.9.5.3 Planned versus actual delivery timelines;

7.9.5.4 Defect management and resolution status;

7.9.5.5 Technical improvements implemented;

7.9.5.6 Outstanding development activities, dependencies and risks;

7.9.5.7 Progress against agreed improvement initiatives; and

7.9.5.8 Recommendations for future system enhancements.

7.9.6 Testing and Quality Assurance Reporting - Service provider should describe the testing and quality assurance reporting processes that will be applied before implementation of changes into the production environment, including;

7.9.6.1 Testing activities performed;

7.9.6.2 Unit testing, system testing, integration testing, regression testing, performance testing and security testing where applicable;

7.9.6.3 User Acceptance Testing (UAT) support and outcomes;

7.9.6.4 Test results and quality assessment reports;

7.9.6.5 Outstanding defects and their impact on implementation;

7.9.6.6 Confirmation of readiness for production deployment; AND

7.9.6.7 Quality improvement recommendations.

7.9.7 Release and Deployment Reporting - Service provider should describe the reporting that will be provided for system releases, upgrades and production deployments, including:

7.9.7.1 Release schedules and implementation plans;

7.9.7.2 Release readiness assessments;

7.9.7.3 Confirmation that required approvals and testing have been completed;

7.9.7.4 Production deployment activities;

7.9.7.5 Deployment outcomes and post-implementation verification;

7.9.7.6 Rollback activities where applicable;

7.9.7.7 Post-release monitoring; and

7.9.7.8 Lessons learned and improvement actions.

7.9.8 Executive Reporting - Service provider should describe the proposed executive reporting approach, including:

7.9.8.1 Roles and responsibilities of governance participants;

7.9.8.2 Service management structures;

7.9.8.3 Escalation and decision-making processes;

7.9.8.4 Engagement model with NT business stakeholders and NTICT;

7.9.8.5 Change governance processes;

7.9.8.6 Risk and issue management processes; and

7.9.8.7 Governance reporting mechanisms

7.9.9 Review meetings - Service provider should recommend the frequency, format and participants for service review meetings, including:

7.9.9.1 Operational review meetings;

7.9.9.2 Monthly service management meetings;

7.9.9.3 Quarterly governance meetings; and

7.9.9.4 Executive review meetings and any other governance forums recommended by the Service provider.

7.9.10 Performance measurement - Service provider should recommend appropriate performance measures and Key Performance Indicators (KPIs) for monitoring service delivery, including:

7.9.10.1 System availability and reliability;

7.9.10.2 Incident response and resolution performance;

7.9.10.3 Change success rate;

7.9.10.4 Release quality;

7.9.10.5 Defect trends;

7.9.10.6 Enhancement delivery performance;

7.9.10.7 Customer satisfaction;

7.9.10.8 Security and vulnerability remediation performance;

7.9.10.9 Capacity and performance trends; and

7.9.10.10 Continuous improvement achievements.

7.10 Technical Management and Continuous Improvement Reporting

7.10.1 For purposes of this section, the term "technical debt" refers to legacy components, outdated technologies, recurring technical issues, system limitations, maintenance requirements and other areas requiring technical improvement, remediation or modernisation to ensure the continued reliability, security, performance and sustainability of the SafetyWeb Banking System.

7.10.2 Service providers should describe their approach to identifying, managing and addressing technical debt as part of the ongoing maintenance, support, enhancement and further development services included in the fixed monthly service fee.

7.10.3 Service provider should confirm how technical debt will be proactively managed and addressed throughout the contract period as part of the managed service and without additional charges outside the agreed fixed monthly fee. The response should include, but not be limited to:

7.10.3.1 Identification of legacy components, outdated technologies, recurring issues, system limitations and areas requiring improvement;

7.10.3.2 Recommendations to im[1]prove system performance, security, resilience, maintainability and sustainability;

7.10.3.3 Planned remediation activities and enhancement initiatives;

7.10.3.4 Progress reporting on improvements implemented;

7.10.3.5 The impact of unresolved technical debt on the SafetyWeb Banking System; and

7.10.3.6 Continuous improvement initiatives to ensure the long-term effectiveness and sustainability of the system

7.11 Innovation and Industry Best Practice - Service provider should identify:

7.11.1 Opportunities to improve the current environment;

7.11.2 Innovative technologies that could enhance the SafetyWeb Banking System;

7.11.3 Best practices for supporting mission-critical banking applications;

7.11.4 Recommendations to improve system resilience, security, performance and maintainability; and

---

1

7.11.5 Approach to continuously reviewing, improving and enhancing the payment validation, fraud prevention and transaction monitoring capabilities of the SafetyWeb Banking System in response to emerging fraud threats, changes in payment practices and evolving cybersecurity risks.

7.12 Commercial Information and Pricing Model

7.12.1 The NT is the owner of the SafetyWeb Banking System and requires a comprehensive managed service model based on a fixed monthly fee arrangement for the ongoing maintenance, support, enhancement, modernisation and further development of the existing system. The Service provider shall be responsible for delivering all required services, resources and activities necessary to maintain, support and continuously improve the SafetyWeb Banking System within the agreed fixed monthly fee.

7.12.2 Service providers are requested to provide information on their ability to provide a comprehensive managed service through a fixed monthly fee that includes all services required to maintain, support, enhance and ensure the effective operation of the SafetyWeb Banking System.

7.12.3 As part of the managed service, the Service provider shall provide, implement, configure, license (where applicable), maintain and support a call logging and service management system for the duration of the contract. **The call logging and service management system shall form part of the fixed monthly managed service fee, and all associated costs shall be included within the monthly fee. No separate charges shall be applicable for the provision, licensing, operation, maintenance or support of the call logging and service management system.**

7.12.4 The Service provider will be responsible for providing and managing all resources required to deliver the services listed below within the fixed monthly fee, including, but not limited to:

7.12.4.1 Developers, database administrators, technical specialists, systems integration specialists, testing resources, project management resources and other suitably qualified personnel required to maintain, support, enhance and further develop the SafetyWeb Banking System;

7.12.4.2 The ongoing maintenance, support, modernisation and progressive improvement of the existing SafetyWeb Banking System, including the maintenance of legacy application components, remediation of technical debt, implementation of security and technology upgrades, enhancement of existing functionality and development of new functionality approved by the National Treasury;

7.12.4.3 The provision of application support, software development, database administration, technical infrastructure support, systems integration, testing, implementation support, release management and project management services necessary to ensure the continued availability, reliability, security, performance and continuous improvement of the SafetyWeb Banking System; and

7.12.4.4 All maintenance, enhancements, upgrades, new functionality, technical improvements, legislative and regulatory changes, and other approved development activities shall be planned, designed, developed, tested, implemented, documented and supported by the Service provider as part of the fixed monthly managed service fee and in accordance with the NT's approved governance, change management and release management processes.

7.12.5 The fixed monthly managed service fee shall include, but not be limited to, all services, activities, resources and deliverables required to maintain, support, enhance, modernise and ensure the continued effective operation of the SafetyWeb Banking System, including:

7.12.5.1 Application maintenance and support, including corrective, preventative, adaptive and perfective maintenance;

7.12.5.2 Incident, problem, request, change and release management services;

7.12.5.3 Provision, implementation, configuration and management of a call logging and service management system;

7.12.5.4 System enhancements, improvements, further development and modifications required by the NT;

7.12.5.5 System upgrades, including application, database, security, framework, middleware and related technical upgrades required to maintain a secure, supported and effective operating environment;

7.12.5.6 Development and implementation of new functionality, features, integrations, reports and modifications required to meet changing business, legislative, regulatory and operational requirements;

7.12.5.7 Maintenance, enhancement and improvement of payment validation, transaction verification and fraud prevention controls within the SafetyWeb Banking System;

7.12.5.8 Database administration and support, including performance tuning, optimisation, integrity management, backup and recovery support;

7.12.5.9 Technical environment support, including application server, web services, Connect, integration and related technical components;

7.12.5.10 Coordination and support of infrastructure-related activities with NTICT, including server configuration, vulnerability remediation, performance monitoring and technology upgrades;

7.12.5.11 Software development lifecycle activities, including requirements analysis, design, development, testing, documentation, deployment and post-implementation support;

7.12.5.12 Project management, service management, reporting, governance and stakeholder engagement services;

7.12.5.13 Technical debt management, modernisation activities and continuous improvement initiatives required to improve the resilience, security, maintainability and sustainability of the SafetyWeb Banking System; and

7.12.5.14 Any other activities, resources or services reasonably required to ensure the continued availability, reliability, security, performance and continuous improvement of the SafetyWeb Banking System.

7.12.6 Risks and Challenges

7.12.6.1 Service providers are requested to identify and describe the key risks and challenges associated with providing maintenance, support, enhancements and further development services for a mission-critical government banking system such as SafetyWeb

7.12.6.2 Service provider should provide recommendations on how these risks can be effectively managed and mitigated throughout the contract period. The response should include, but not be limited to, the following:

7.12.6.2.1. Risks associated with the continuous availability of the SafetyWeb Banking System;

7.12.6.2.2. Risks relating to payment processing and the timely resolution of critical incidents;

7.12.6.2.3. Cybersecurity and information security risks, including vulnerability management and protection of sensitive banking information;

7.12.6.2.4. Risks associated with system upgrades, enhancements and production deployments, together with proposed mitigation measures;

7.12.6.2.5. Risks relating to system integrations and interfaces with external stakeholders, including the South African Reserve Bank, commercial banks and other government systems;

7.12.6.2.6. Risks associated with database integrity, backup, recovery and disaster recovery;

7.12.6.2.7. Resource availability, succession planning and retention of critical technical skills;

7.12.6.2.8. Risks associated with business continuity and service delivery during periods of increased operational demand;

7.12.6.2.9. Risks relating to change management and the implementation of new functionality;

7.12.6.2.10. Risks associated with compliance with government policies, standards and security requirements;

7.12.6.2.11. Any other risks that service provider consider relevant to the successful delivery of the required services; and

7.12.6.2.12. Risks associated with maintaining effective payment validation, fraud prevention and transaction monitoring controls, including emerging fraud techniques, evolving payment practices and cybersecurity threats.