South African Reserve Bank

Financial Services Department - Procurement Section
370 Helen Joseph Street (formerly Church Street)
Pretoria

Request for Proposals - RFP No GvdW/02-2013

Appointment of a service provider to provide Security and Penetration Testing and Assessment services, relating to the Web-based SAMEXWeb application and related components, within the South African Reserve Bank.

Date of issue 31 March 2013

Closing date: Friday 12 April 2013 – 12h00

State full name of organisation/individual:

State discipline

Contents

Invitation for Proposals

Invitation

The South African Reserve Bank (the Bank) wishes to appointment a service provider to provide Security and Penetration Testing and Assessment services, relating to the Bank's Web-based SAMEXWeb application and related components, as detailed in Section 3 of this document. The Bank accordingly invites your organisation as a potential service provider to take part in the Request for Proposal (RFP).

Potential service providers must kindly take note that the Bank is a National Key Point and as such short-listed service providers will be subjected to extensive security vetting as dictated by the enabling legislation and to the acceptance of a Confidentiality Agreement. It is the preference of the Bank to only use South African Citizens.

Proposal documents together with five (5) copies clearly marked "original proposal" and "copy", as well as an electronic copy of your proposal will be received until **12h00 on Friday 12 April 2013** and must be enclosed in sealed envelopes, bearing the applicable tender headings, tender reference number as well as the closing time and due date, as per the supplied cover page of this document.

The proposals should be deposited in the tender box situated at the South African Reserve Bank, Head Office, 370 Helen Joseph Street, Pretoria, for attention Gerda van der Walt. Proposals shall remain valid for a period of 120 (one hundred and twenty) days from the closing date for the submission of tenders, during which period it may not be amended or withdrawn.

Late submissions will not be considered.

Section 1: Conditions of Proposal

1.1 Introduction

1.1.1 The Bank will select organisation(s) among those short-listed from the invitation.

1.1.2 Please note that (i) the costs incurred or losses suffered by the service provider in preparing and submitting a proposal and negotiating the tender, including visits to the Bank premises, are not reimbursable as a direct cost of the assignment; and (ii) the Bank is not bound to accept any of the proposals submitted.

1.1.3 The Bank policy requires that the service providers to provide professional, objective, and impartial advice and at all times hold the Bank's interests paramount, without any consideration for future work.

1.1.4 It is the Bank's policy to require that service providers observe the highest standard of ethics during the execution of such RFP's. The Bank will reject a proposal for award if it determines that the service provider recommended for the award has engaged in corrupt or fraudulent activities in competing for the project in question.

1.2 Clarification and amendment of the proposal documents

1.2.1 Service providers may request a clarification of any information in the proposal before the submission date. Any request for clarification must be sent in writing (by e-mail) to the following person at least 48 hours before the closing date:

Mrs Gerda van der Walt, telephone number: 012-313 3787, 012-313 3426 or

E-mail to Gerda.vanderwalt@resbank.co.za

1.2.2 The Bank may, for any reason, whether at its own initiative or in response to a clarification requested by an invited service provider, amend the proposal. Any amendment shall be issued in writing through addenda.

1.2.3 Addenda shall be sent by fax or e-mailed to all invited service providers and will be binding on them. The Bank may at its discretion extend the deadline for the submission of proposals.

1.3 Preparation of proposal

1.3.1 Service providers are requested to submit a proposal written in English.

1.3.2 In preparing the proposal, service providers are expected to examine the documents constituting this proposal in detail. Material deficiencies in providing the information requested may result in rejection of a proposal.

1.3.3 While preparing the proposal, service providers must ensure that the majority of the key professional staff proposed has a proven, extended and stable working relationship with them.

1.3.4 Service providers may act as a consortium with other service providers to respond to the RFP. However, a primary service provider must act as the respondent and it will be the primary service provider's responsibility to negotiate and conclude relationships with any other service providers.

1.4 Submission of proposal

1.4.1 Service providers must note that if the conditions set out hereafter are not closely adhered to it may result, at the sole discretion of the Bank, in the proposal not being accepted for consideration.

1.4.2 The original proposal shall contain no inter-lineation or overwriting, except as necessary to correct errors made by the service provider. Any such corrections must be initialled by the person or persons who sign(s) the proposals.

1.4.3 Proposals have to be submitted on the official forms included in the proposal documents and preferably not be qualified by the service provider's own conditions of proposal**.**

1.4.4 Each service provider is required to return the complete set of proposal documents, which was obtained from the Bank, with all the required information supplied and completed in all respects.

1.4.5 Service providers are requested to supply all information requested in the RFP.

1.4.6 Service providers are instructed to adhere strictly to the numbering used in the proposal document to facilitate ease of evaluation.

1.4.7 Service providers are to note that it remains the responsibility of the tenderers to ensure the **timely** delivery of the proposal.

1.5 Completion of proposal

1.5.1 The forms included in these proposal documents are drawn up so that essential information has to be furnished. The proposal document contains forms of tender to be completed by the service provider in every detail, in ink.

1.6 Signing of proposal

1.6.1 The person duly authorised thereto shall sign the proposal.

1.7 Publicity and media releases

1.7.1 While the RFP process is in progress, the service provider is not entitled to generate publicity or issue media releases that in any way refer to this RFP or the service provider's response to it, without the prior written consent of the Bank.

1.8 Procurement process

1.8.1 This is the proposal stage of the procurement process.

1.8.2 Prior to the submission of your RFP response, potential respondents may request a clarification of any information in the proposal before the submission date. Any request for clarification must be sent in writing (by e-mail) at least 48 hours before the closing date.

1.8.3 The Evaluation Committee will evaluate the proposals on the basis of the evaluation criteria. Each proposal will be awarded a score.

1.8.4 A proposal shall be rejected at this stage if it does not respond to important aspects as set out in the RFP or if it fails to achieve the minimum score pre-determined by the Evaluation Committee.

1.8.5 The **estimated** dates for the procurement process is as follows:

- RFP issued - 31 March 2013
- RFP close - 12 April 2013 at 12:00

1.9 Requirements

1.9.1 Only companies that can provide **evidence** of the following minimum criteria need to respond:

1.9.1.1 A minimum of 5 years of security / penetration testing of high value Web-based systems in the South African financial industry,

1.9.1.2 A local skills base of specialist testers with CISSP (Certified Information Systems Security Professional) and CEH (Certified Ethical Hacker) accreditation and at least 3 years relevant experience in penetration testing, and

1.9.1.3 Accreditation with multiple industry organisations including CREST and PCI ASV and / or PCI QSA (as defined in 1.9.2.1).

1.9.2 Potential service providers will be required to meet the following minimum criteria:

1.9.2.1 Industry accreditations

- CREST Accredited member Company
  "CREST provides demonstrable assurance of the processes and procedures of member organisations and validates the competence of information security testers”

- PCI "ASV" or "QSA" Company Accreditation
  ASV: "Approved Scanning Vendors (ASVs) are organizations that validate adherence to certain PCI DSS (Data Security Standard) requirements by performing vulnerability scans of Internet facing environments of merchants and service providers".

  QSA: "Qualified Security Assessor (QSA) companies are organizations that have been qualified by the Council to have their employees assess compliance to the PCI DSS standard."

- Testers should be both CISSP and CEH certified.
  CISSP: "Certified Information Systems Security Professional (CISSP) is an independent information security certification governed by International Information Systems Security Certification Consortium also known as $(ISC)^2$."

  CEH: "The Certified Ethical Hacker is a professional certification provided by the International Council of E-Commerce Consultants (EC-Council.)"

- All testers must have more than 3 year’s demonstrable experience with penetration testing.

- **Evidence** must be provided that the testers proposed are proficient in the security testing and assessment disciplines related to this tender and in terms of the industry accreditations listed above.

1.9.2.2 Proven company experience of prior Web-based systems Security Testing in the South African financial industry, with at least two contactable references.

1.10 Proposal evaluation criteria

1.10.1 Proposals will be evaluated based on the following criteria inter alia;

- Company profile which contains commercial requirements such as tax clearance certificate, certificate of incorporation,
- Compliance to Broad Based Black Economic Empowerment initiatives,
- The proposed fee structure,
- Core competency,
- Client base,
- Evidence of company accreditation,
- Proven track record and experience in the field of web-based systems security testing,
- Company references (proven track record and expertise in similar projects,
- Capacity and expertise to deliver the requirements included in the scope with relevant curriculum vitae,
- Ability to provide local skills proficient in the security assessment disciplines related to this tender and in terms of the industry accreditations stated,
- An understanding of the South African acts and regulations
- Security testing approach and reporting (recommendations, etc.), and
- CV’s of the proposed task team (testers).

1.11 Negotiations

1.11.1 Negotiations will include a discussion of the proposal. The Bank and the service provider will work out final Terms of Reference indicating activities, staff, logistics and reporting. The agreed programme and final Terms of Reference will then be incorporated in the “Description of Services” and will form part of the agreement.

1.11.2 Special attention will be given to getting the most the service provider can offer, the best value for money within the available budget and to clearly define the inputs required from the Bank to ensure satisfactory results.

1.12 Awarding the tender

1.12.1 The tender will be awarded following negotiations. After successful negotiations, the Bank will promptly notify other service providers on the shortlist that they were unsuccessful. The appointed service provider is expected to commence on the date as agreed upon with the Bank.

1.12.2 The Bank reserves the right to appoint more than one service provider, to address different sections of the scope, should that be considered in the best interest of the Bank.

1.13 Confidentiality

1.13.1 Information relating to the valuation of the proposal and recommendations concerning awards shall not be disclosed to the service providers who submitted the proposals or to other persons not officially involved in the process, until the successful service provider has been notified that it has been awarded the tender.

1.14 Withdrawal, Substitution and Modification of RFP

1.14.1 The SARB reserves the right to withdraw, substitute or modify the RFP. Notification of any withdrawal, substitution or modification will be given to all vendors.

Section 2: Notes to service provider

2.1 Price to include

2.1.1 The total price shall be deemed to include any and all things and matters necessary for the complete and satisfactory execution and completion of the project whether or not specifically referred to in the document.

2.2 Proposal

2.2.1 The proposal is required to comprise the following:

2.2.1.1 Company profile (including tax clearance certificate and certificate of incorporation),

2.2.1.2 BBBEE details and rating certificate,

2.2.1.3 Section 3 of this document: Scope/specifications and plan of action,

2.2.1.4 Form of Tender (Appendix A),

2.2.1.5 Undertaking of confidentiality (Appendix B),

2.2.1.6 Security vetting documents,

2.2.1.7 Scope of Service Offerings by the Company.

2.3 Quality assurance

2.3.1 The manager of the Bank's Financial Support Services division within the Business Systems and Technology Department will agree with the service provider on set standards of quality acceptance.

2.3.2 Intellectual Property Rights to project material to transfer to the Bank upon the completion of the project.

Section 3: Scope of work

3.1 Background

The Business Systems and Technology department, in conjunction with the National Payment Systems Department within the Bank are seeking the services of a company to provide web-based security and penetration testing and security assessment, on the web-based user interface (SAMEXWeb) for the Bank's current Real Time Gross Settlement System (SAMOS).

3.2 Scope of SAMEXWeb

3.2.1 SAMEXWeb General Architecture Design Overview

The purpose of this section is to provide an overview of the SAMEXWeb solution architecture design. In the interest of positioning the SAMEXWeb solution in relation to the rest of the SAMOS business system, the SAMOS business application and database server is shown as well.

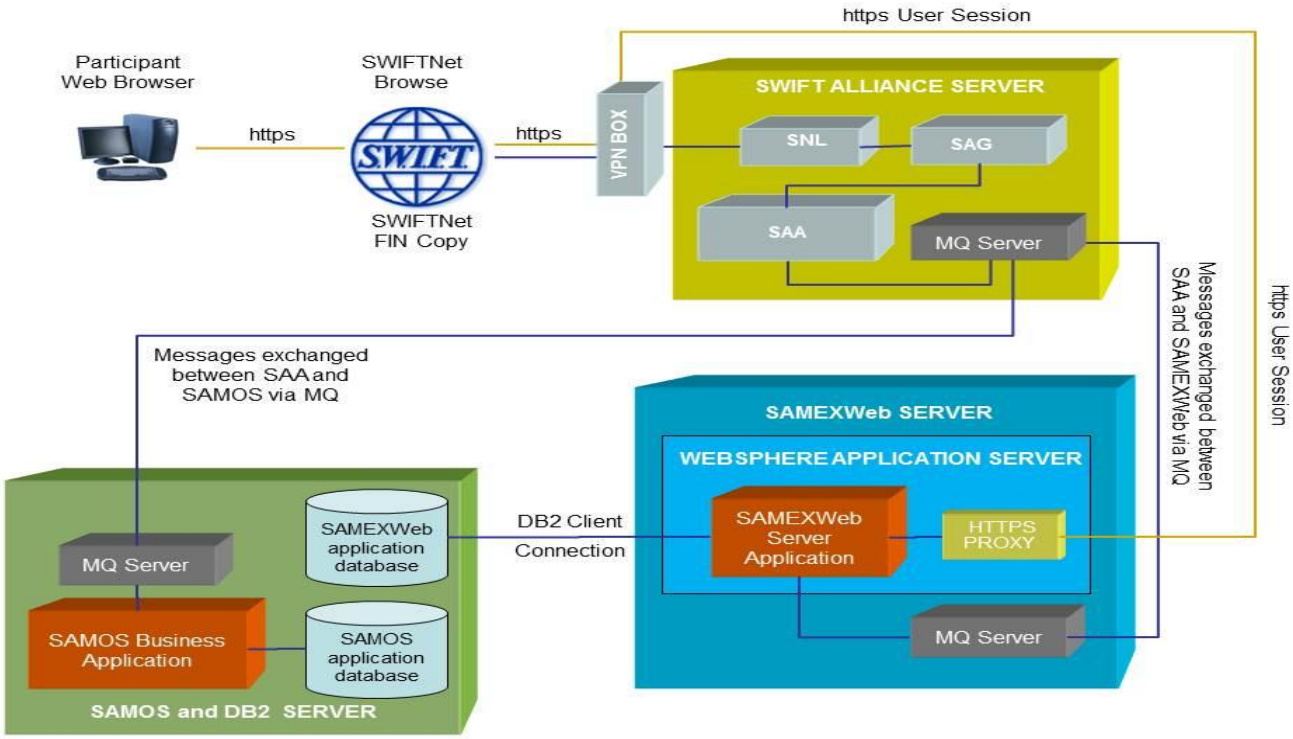


Figure 1 – SAMEXWeb Architecture Logical View

3.2.2 SAMOS Application and Database Server

The SAMOS application and database server hosts the SAMOS core business application and the DB2 database management system on a z/OS mainframe partition.

The DB2 DBMS provides managed access via DB2 client connections to separate database images for the SAMOS application as well as the SAMEXWeb application. The databases and the application binaries are physically located on the Storage Area Network (SAN).

Transactional messages are sent and received by the SAMOS application via MQ and Swift Alliance Access.

3.2.3 SAMEXWeb Application Server

The SAMEXWeb Application Server hosts the SAMEXWeb WAS internet server and J2EE application components on an AIX partition.

The core functions of the SAMEXWeb server is to:

- Integrate with SWIFTNet Evolution in order to authenticate users during the logon process;
- Manage the browser-based sessions with participant users (HTTPS over the SWIFTNet Secure IP Network);
- Provide user authentication and authorisation services;
- Provide the presentation layer and transform business data between the user Web pages and SAMOS message structures; and
- Send and receive business messages to and from the SAMOS application via MQ and Swift Alliance Access.

3.2.4 SWIFT Infrastructure and Alliance Server

The purpose of the SWIFT server is to host the SWIFT software components required to connect to the SWIFTNet SIPN (SWIFT Internet Protocol Network) and send and receive messages to and from SWIFT service offerings.

In the context of the SAMEXWeb sub-system, SAA provides message management and routing services between SAMOS and the SAMEXWeb server application via MQ.

The HTTPS connectivity form the SAMEXWeb user browser is routed via the SWIFTNet VPN box to the HTTPS proxy provided by the WAS environment on the SAMEXWeb application server.

3.2.5 User Authentication and Authorisation

User authentication is implemented using a personalised 2-factor USB token / PKI certificate combination provided by SWIFT under its internal SWIFTNet Certification Authority service, using a SAML Identity Provider service also provided by SWIFT. The SAMEXWeb application integrates with this security infrastructure provided by SWIFT as part of the SWIFTNet Browse Evolution product offering.

User authorisation is based on a proprietary application-level user repository integrated into the SAMEXWeb server application, with distributed management based on segregation of duties and multiple levels of authorisation.

The successful vendor will be provided with additional details and a copy of the SAMEXWeb trust model once the NDA is in place.

3.3 Boundaries of Security Testing

In terms of the SAMEXWeb high level architecture discussed in the previous section, the following components fall within the scope of this RFP:

- The HTTPS connectivity between the end user browser and SAMEXWeb application server;
- The SAMEXWeb application server including all operating system software, application software and configuration files;
- The MQ connections to the SAMOS servers and to the SWIFT Alliance server; and
- The SAMEXWeb DB2 database and the client connection to DB2 from the SAMEXWeb application server.

The analysis and testing of the user sessions will be end-to-end over the SWIFT Secure IP Network and penetration and other testing must be done on the end-to-end user session. However, the SWIFT network, software and services per sé are excluded from the scope of this RFP and the emphasis will be on the integrated end result.

3.4 Security testing requirements

The vendor is required to respond to each of the requirements individually, supplemented where necessary with additional material appended to the RFP response.

3.4.1 Scope

3.4.1.1 Security testing must be done at the Application Layer and the Infrastructure Layer.

3.4.1.2 Testing should include Authenticated and Unauthenticated ('black box') testing.

3.4.1.3 The SAMEXWeb application source code must be reviewed, as well as other data sources like architecture documents, trust models, database schematics, directory structures and server log files.

3.4.1.4 Vendors must be able to develop a Threat Model prior to testing, but it must be reflected as an optional separate line item on the cost schedule.

3.4.1.5 All security testing will be done from the offices of the SA Reserve Bank in Pretoria.

3.4.1.6 The successful vendor will be expected to perform a re-test to verify that identified issues have been addressed, as a separate line item on the cost schedule.

3.4.1.7 The successful vendor will be expected to perform a post-production 'regression' test, in order to verify that no new issues/threats have been introduced into the production environment. This activity must be shown as a separate line-item on the cost schedule.

3.4.1.8 The SAMEXWeb system is expected to go live mid-October 2013 and will be available for the security testing sequence from late April 2013. Vendors must state their ability to provide the expected services within these time frames.

3.4.1.9 Vendors must describe the extent to which to which the potential perceived threats in the table below will be addressed. The list of threats is not exhaustive and should not be interpreted as a scope definition. Vendors are requested to add additional threats to the table.

Category	Threats / Attacks
Input Validation	Buffer overflow; cross-site scripting; SQL injection; canonicalization
Authentication	Network eavesdropping ; Brute force attack; dictionary attacks; cookie replay; credential theft
Authorization	Elevation of privilege; disclosure of confidential data; data tampering; luring attacks
Configuration management	Unauthorized access to administration interfaces; unauthorized access to configuration/parameter files/stores; retrieval of clear text configuration data; lack of individual accountability; over-privileged process and service accounts
Sensitive information	Access sensitive data in storage; network eavesdropping; data tampering
Session management	Session hijacking; session replay; man in the middle
Cryptography	Poor key generation or key management; weak or custom encryption
Parameter manipulation	Query string manipulation; form field manipulation; cookie manipulation; HTTP header manipulation
Exception management	Information disclosure; denial of service
Auditing and logging	User denies performing an operation; attacker exploits an application without trace; attacker covers his or her tracks
Penetration testing	Black Box testing (meaning Penetration Testing tools) are ethical hacking tools used to attack the application surface to expose vulnerabilities suspended within the source code hierarchy
Static code analysis	White Box testing give specific visibility into the specific root vulnerabilities within the source code in advance of the source code being deployed

3.4.2 Methodology

3.4.2.1 The vendor must describe the methodology that will be followed in executing the security assessment testing. The framework that follows is not prescriptive, but the responses must clearly indicate how the elements of the framework will be addressed:

a. **Understanding phase**: Review of design documentation, discussions with architects, designers, administrators and/or developers;

b. **Threat model phase:** Design a threat model based on the system design constructed in the Understanding phase;

c. **Vulnerability discovery phase:** Reconnaissance, footprinting, vulnerability scanning;

d. **Web application discovery phase:** Enumeration and ranking of the SAMEXWeb application aspects, including:

i. Surveying the application

ii. Authentication

iii. Authorisation

iv. Session and State Management

v. Input Sanitation

vi. Business logic flaws from the security perspective; and

e. **Exploitation phase**: Verification of vulnerabilities identified either through the threat model or the vulnerability discovery phase.

3.4.2.2 Vendors must describe the methodology proposed to assess the MQ component.

3.4.2.3 Reports and test results must be provided in writing and must be presented in a workshop or a series of workshops. Testers will be expected to explain

their findings and incorporate feedback into a revised report as may be appropriate. The reports and test results must include elements related to:

a. Technical, System and Management;

b. Attack trees where appropriate;

c. Detection and response actions on threats where appropriate.

3.4.3 Skills and Qualifications

3.4.3.1 The vendor must provide an overview of its internal controls or system for rating and grading testers and insuring quality control.

3.4.3.2 The testers proposed by the vendor:

- Must be individually identified and named in the response;
- Must have a minimum of 3 years relevant experience;
- Must gave demonstrable skills in the required areas;
- Must have relevant basic formal certifications such as CISSP, CERT, SANS, CEH, PCI ASV / QSA; and
- Must provide a CV with customer referrals and/or case studies.

3.4.3.3 The vendor must identify areas where the vendor is leading the industry and provide evidence of same.

3.4.3.4 The vendor must demonstrate that it will have the appropriate skills available to respond to the needs and time lines of this RFP.

3.4.3.5 The vendor must state whether sub-contractors will be used. The preference of the SARB is that only permanent employees of the vendor should be used.

3.4.3.6 The vendor is required to provide a sample report relevant to the subject matter of this RFP. References to existing or past customers may be removed.

3.5 Timeframe (estimated)

3.5.1 First security test to be conducted in the testing environment during the period of 18 June to 1 July 2013

3.5.2 Second security test to be conducted in the testing environment during the period of 29 July to 12 August 2013

3.5.3 Third and final security test to be conducted in the quality assurance testing environment during the period of 2 to 16 September 2013

3.5.4 Service Providers will be appointed as preferred suppliers for a period of 3 years renewable annually.

3.5.5 Service Providers will be required to provide their standard contract with terms and conditions in your response to this proposal.

3.6 Completion of the RFP Response

3.6.1 For ease of reference and evaluation, your RFP response must use the same reference numbers included in Section 3

3.6.2 All cost estimates should be provided on a fixed price basis

3.6.3 You are hereby invited to submit your proposals for the requirements detailed in section 3.

Section 4: Breakdown of costs

Cost breakdown and resource allocation according to the relevant fees, and including VAT must be attached hereto, and both the breakdown and Appendix A must be signed by the service provider.

The cost breakdown and resource allocation should be submitted on the company letterhead and should be signed by the authorised signatory.

Signed: _____

(for and on behalf of the service provider who by signature hereof warrants authorisation hereto)

Date: _____

Section 5: Summary of conditions of contract

5.1 Conditions of contract

Some of the terms of the contract which shall govern the rendering of services are set out herein below. However, the Bank may draft comprehensive conditions of contract after awarding the tender, if deemed necessary. The Bank is agreeable to negotiate the terms and conditions of the contract as may be reasonably required by either the Bank or the Service Provider.

5.2 Contact person

The Service Provider is to ensure that a contact person is appointed to the Bank's project.

5.3 Cost

It is the service provider's responsibility to ensure that the cost tendered, includes all matters deemed necessary for the successful execution of the project.

5.4 Insurance

The Service provider is to insure their own personnel, equipment and vehicles.

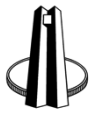
5.5 Protection of the service

The Service Provider must warrant the rendering of the service to the Bank for the period of the contract.

5.6 Contract type

Kindly supply an example of your proposed service contract.

Appendix A: Form of Tender



South African Reserve Bank

Appointment of a service provider to provide Security and Penetration Testing and Assessment services, relating to the Web-based SAMEXWeb application and related components, within the South African Reserve Bank.

Employer: The South African Reserve Bank

Street address: 370 Helen Joseph Street, Pretoria

Telephone number: 012-313 3787

Service provider: _____

Contact person: _____

Postal address: _____

Telephone: _____ Fax: _____

E-mail: _____

Proposed tender sum			
14% VAT (if applicable)			
Total:			

Amounts in words

_____

_____

Signed: _____

(for and on behalf of the service provider who by signature hereof warrants authorisation hereto)

Date: _____

Vat registration number: _____

Kindly attach a copy of your standard contract for these services

South African Reserve Bank

Appendix B: UNDERTAKING OF CONFIDENTIALITY

This undertaking of confidentiality is made and entered into on this ____ day of _____ 2013, by _____ (insert full names) in his / her capacity as (insert) of (insert name of institution and registration number, where applicable), with its usual place of business at _____(insert), hereinafter referred to as the "recipient", in favour of the South African Reserve Bank, hereinafter referred to as the "SARB", with its usual place of business at 370 Helen Joseph Street, Pretoria.

In consideration of the mutual covenants and provisions contained herein, the recipient undertakes as follows:

In this agreement, the following terms will have the meanings ascribed to them below:

"effective date" shall mean the date upon which this agreement is signed;

"SARB" shall mean the party making information, as defined below, available to the other party;

"recipient" shall mean the party to whom information, as defined below, is made available;

"information" shall include:

Information relating to the feasibility project;

Data furnished, disclosed and/or transmitted to the recipient, whether disclosed orally or in writing, which is clearly identified by the SARB as being confidential; and

Notes, analyses and other documents prepared by the recipient or its representatives which have been based upon or derived from confidential information received from the SARB.

"product/service" shall mean the feasibility project and services described in this RFP.

In furtherance of this agreement, the SARB may, at its option, make information available to the recipient. Information disclosed verbally, in writing or electronically will be considered as confidential. However, information shall not include any information which:

Is contained in a publicly available printed publication prior to the date of this agreement;

Is or becomes publicly known through no wrongful act on the part of the recipient;

Is known by the recipient without any proprietary restrictions at the time of receipt of such information from the SARB or becomes known to the recipient without proprietary restrictions from a source other than the SARB; or is independently developed by the recipient without reference to the information disclosed by the SARB.

The recipient agrees to receive the information in the utmost confidence and to keep the same information confidential, using at least the same degree of care as is used by the recipient to protect its own confidential information.

The recipient further agrees to disclose the information only to its authorized employees, sub-contractors, suppliers, legal advisors and financial advisors whose services are required in

furtherance of the objectives of the business relationship between the parties, and to require each of its colleagues, and its authorized employees, sub-contractors, suppliers, legal advisors and financial advisors to comply with the terms of this agreement, prior to the disclosure to such employees, sub-contractors, suppliers, legal advisors and financial advisors.

The recipient shall not make any additional copies of information without the express written consent of the SARB. The recipient, will at its own cost, and after a written request has been submitted by the SARB, return all documents and tangible property in its possession which contain any part of the information disclosed to the recipient by the SARB hereunder.

The recipient shall use such information only in connection with the furtherance of the business relationship between the parties, and the recipient shall make no further use, in whole or in part, of any such information. However, nothing in this agreement shall restrict the SARB from using, disclosing or disseminating its own information in any way.

The recipient shall not be entitled to utilize the name of the SARB in publicity releases, advertising or for other promotional purposes without securing the prior written consent of the SARB.

The obligations imposed by this agreement will remain in perpetuity.

This agreement sets forth the entire agreement and understandings between the recipient and the SARB (the ‘‘parties’’) as to the subject matter hereof and supersedes, cancels, and merges all agreements, negotiations, commitments, writings, and discussions between them as to the subject matter prior to the date of this agreement. Neither of the parties shall be bound by any condition or representations with respect to such subject matter, other than as expressly provided in this agreement or as duly set forth on or subsequent to the date of this agreement in writing, and signed by a proper and duly authorized representative of the parties.

This agreement will be governed by and construed in accordance with the law of the republic of South Africa and the parties agree to submit to the exclusive jurisdiction of the South African courts.

In the event of the invalidity or unenforceability of any provision of this agreement under any applicable law, the parties agree that such invalidity or unenforceability shall not affect the validity or enforceability of the remaining portions of this agreement.

In witness whereof the recipient has caused this agreement to be signed in its name.

_____
Signature of recipient on behalf of the organization referred to at the beginning of this agreement, who by affixing his/her signature hereto warrants his/her authority to bind the organization.

_____
Name

_____
Title

_____
Date

South African Reserve Bank

Appendix C: Security Vetting

Please note that each company, consultant and or contractor appointed by the Bank will be subjected to a personnel security vetting process in accordance with the Bank's Security Vetting Policy. Companies, consultants and contractors must submit copies of the following documentation.

1 Documents to be submitted with regard to the Company

1.1 Company name and registration number;

1.2 A valid Tax Clearance Certificate - Tender (not older than 6 months);

1.3 A certified copy of a valid certificate to commence business;

1.5 A certified copy of a valid certificate of change of name of company;

1.6 A certified copy of a valid certificate of incorporation of a company having a share capital;

1.7 A certified copy of the JV agreement;

1.8 A certified copy of Professional Indemnity Insurance Cover;

1.9 A list reflecting the names and ID numbers of all the company directors; and

1.10 A company profile.

2 Documents to be submitted with regard to consultants/contractor or staff

2.1 A list reflecting the names, ID numbers and a short description of the role of each staff member on the project.

2.2 A certified copy of the first page of the ID book of each staff member on the project.

3. Security Vetting Process

As the Bank is an organ of state and a National Key Point, the National Intelligence Agency is obliged to issue all Bank employees (permanent and temporary employees of the Bank, job applicants, independent contractors or contract workers, consultants, and other service providers) with a security clearance. Through personnel security vetting, the Bank ensures that all employees have appropriate security clearances for the work they are required to do.

The personnel security vetting process is guided by the principles of fairness, objectivity, professionalism, respect for human rights and privacy, and the application of due processes as enshrined in the Bill of Rights, Chapter II of the Constitution of the Republic of South Africa (Act No 108 of 1996). In particular, the employee's right to privacy, religion, belief, opinion, freedom of expression, freedom of association, freedom of movement and residence, and political rights will be duly respected by the Bank.

All the individuals that you may require for the purpose of this project will have to complete a security clearance questionnaire and be successfully security cleared prior to accessing any Bank premises or information.