TERMS OF REFERENCE
for
Security Assessment ofDa Afghanistan Bank(DAB) IT Infrastructure

1. Background

Da Afghanistan Bank, the Central Bank of Afghanistan, established the Information Technology Department in 2005 to create a technological base for DAB departments' automation and integration with the operating branches to have integrated financial system. The purpose of establishing IT department was to enable the technically strengthened DAB to further enhance its reach and capability towards achieving the strategic goals and objectives.

Following the Kabul Bank crisis in the end of 2010 the Government of Afghanistan approached the international community, led by the IMF, to assist the Government in stabilizing and strengthening the banking sector and laying the foundation for banking sector development in the country. The World Bank provided positive response to the request of the Afghan Government by designing a project called the **Strengthening Afghanistan Financial Intermediation Projecte (SAFI)** focusing on a set of selected activities that would help restore public confidence in the strengthened and secured banking sector.

1.1. Keeping the objectives of **SAFI** in mind, the need was felt by the organisation to periodically conduct information security assessment of their environment which was driven by two factors:

- The increasing level of threats from internal users fromexternal hackers could come through compromised internal users
- The growing commercial imperatives for compliance with data security, accessibility and retention standards

Benefits of information security assessment include:

- Identify gaps in organisational security controls, policies and processes.
- Discover the risks of external and internal security threats to organisations and provide detailed recommendations to mitigate them.
- Improve organisations overall security posture and productivity based on recognised business needs.
- Understand clearly the security issues and requirements within organisations information systems or applications before they are exploited.
- Provide secure environmentfor business applications especially critical and core business applications.
- Increase trust and confidence in the organisations systems and applications by ensuring the secure availability of their information systems or applications for their customers.

1.2Security assessment is a key and critical factor for the financial sector and majority of the investment is on the infrastructure security. So this assessment is very important for Central Bank to identify the security risks and respondwith a valid and right-sized solution.

The information technology department applied several security measures to the DAB IT Infrastructure

a. Establishment of security section within the IT department
b. Prepared different IT security policies and procedures
c. Several other technical and logical security measures within the infrastructure
d. Conducted basic security trainings and awareness programs
e. Segregation of User management from Operational departments.

2. Objective

The objectives of the assessment are:

a. Ensure adequacy of the cyber-risk and IT security risk managementof DAB's Information Technology infrastructure, platforms and ATS (RTGS, ACH & CSD), the Core Banking System (CBS), the Financial System (ERP),the National Switch (APS) and all current applications of DAB through:an assessment of the current security measures and recommendationstoDAB with the right solution in order to increase the risk managementmeasures to international best standard ~~(ISO 27001)~~.

b. The Information Security (IS) and cyber security risk Assessment will entail conducting a risk assessment of the IS Systems at the Bankincludingidentification and evaluation of the risks and method of mitigation of such risks. In the light of the risk assessment exercise, the selected consulting firms should recommend and assist in implementing a set of international best practices governing the Management of Information Systems in the Banking Sector world-wide. The Consultant shall also assess the compliance of the regulatory standards.

In order to achieve the above objectives, DAB is looking for qualified and competent firms who have enough experience in security assessment and possess the required security and ISO certification to do the said security assessment with their certified information security staff and toolsFor Developing of Cyber Security policy using ISO/IEC 27032.

3. Scope of Services,

The scope of this assignment involves a comprehensive review of the Afghanistan Bank applications, the database, network infrastructure, physical security and procedures, all data centers (Production, Near DR and far DR) this review will include but not limited to:

Phase One:

1. External network Vulnerability Assessment and Penetration Testing
2. Internal Network Vulnerability Assessment and Penetration Testing
3. Internal Web Application Penetration Testing
4. Synthetic transaction Testing
5. Misuse case testing
6. DMZ or Network Architecture Designs / Reviews
7. Server Security and Configuration Reviews
8. Database Security and Configuration Reviews
9. Firewall and Router Configuration Review
10. Data Centers Security
11. VPN Configuration Reviews
12. Third Party Interconnection Review
13. Application Security Configuration Review
14. Back up and restoration policy and procedure review

15. Incident Response Program Development or Review
16. System Configuration and Change Management Review
17. ISO 27001, PCI DSS, Swift CSP and CPMI-IOSCO cyber risk guidanceGap Analysis
18. Security review of the application through Wide Area Network (WAN)
19. Examining various components of the security including data security, application systems security, different systems and facilities and people security
20. Assessment of the adequacy of controls and procedures that identify an individual when transacting business through ICT Channel
21. Effectiveness of controls for managing performance and capacity that satisfy the business requirements.
22. Assessment of the adequacy of controls over the use of various devices
23. Assessment of the adequacy of policies, procedures and controls that ensure that records created and information captured are authentic and reliable
24. Assessment of whether all significant risks within the applications operations management, including continuity of systems are adequately and effectively controlled
25. Assessment to determine whether significant risks within the system have been identified by management and controls are in place over those risks.
26. ReviewBusiness impact analysis and Business Continuity Plan (BCP) including BCP test procedures and planning.
27. Developing IT and cyber security Security Assessment framework for DAB
28. Developing Cyber Security Policy for DAB
29. Assessment and review of Systems/Serverssecurity
30. Assessment of Near and Far Disaster Recovery Sites of Da Afghanistan Bank
31. Assessment of System configurations and System architecture
32. Pre assessment of DAB infrastructure for the implementation of new CBS and ATS
33. Assessment of current information security governance and Information security budget allocation process
34. Assessment of Emailsecurity , remote access and endpoint security assessments for good overall defense in depth security posture.

The firm is required to do the information security assessment of DAB's infrastructure with internationally approved standard tools and procedure. The following are the minimum requirement for information security assessment, which have to be done by the Consulting firm but not limited to the following.

35. Operating System (OS) for servers, Databases, network equipment, Security Systems, Storage Area Networks.

    a. Set up and maintenance of system parameters
    b. Patch Management
    c. Change Management Procedures
    d. Logical Access Controls
    e. User Management & Security

f. OS Hardening
g. Performance, Scalability and Availability

36. **Review of IT Processes and IT Management Tools**
    a. IT Asset Management
    b. Enterprise Management System
    c. Help Desk
    d. Change Management
    e. Incident Management
    f. Network Management
    g. Backup & Media Management
    h. Enterprise Anti-Virus Management
    i. Vendor & SLA Management

37. **Security Management**
    a. Security Equipment Configurations & Policies
    b. Penetration testing and Vulnerability Assessment (PT / VA) of various securityzones.

38. Vulnerability Assessment and Penetration Testing

    Gray Box Penetration Testing
    Active Assessment and Penetration Testing
    External Assessment and Penetration Testing
    Host-Based Assessment and Penetration Testing
    Application Assessments and Penetration Testing
    Passive Assessment and Penetration Testing
    Internal Assessment and Penetration Testing
    Network Assessment and Penetration Testing
    Wireless Network Assessments and Penetration Testing
    Examine and evaluate Physical Security
    Footprinting and Reconnaissance
    Web Server Assessment and Penetration testing
    Review Cryptography
    Web Application Assessment and Penetration testing
    DHCP and Domain Assessment and Penetration Testing
    Review and checking Physical Network Security Design
    Scan Beyond IDS and Firewall
    Perform Banner Grabbing/OS Fingerprinting
    Application Debug Scanning
    Scanning Buffer Overflows
    Scanning Operating System Flaws

38. **Network& systems assessment**
    a. Network architecture review
    b. Network traffic analysis and base lining
    c. Network Security review and providing recommendations for better security configuration

39. **Develop and prepare the following policies:**
    Review and provide the policy documents such as Contingency Planning, Risk Management Document, Cyber Security Policy and Cyber security framework/policy which will be applied to all commercialbanks,data centre policy and control standard checklist, incident management policy, and data classification policy etc.

40. **Address Common Vulnerabilities in E-commerce Environments**

Vulnerabilities Caused by Insecure Coding Practices (Cross-site Scripting (XSS),SQL Injection Flaws, Cross-site Request Forgery (CSRF), Buffer Overflows, Weak Authentication and/or Session Credentials.

b. To carry out ASV Scanning of Web-hosted Environments, this must be done based on approved policies.

c. Ability to perform technical testing both inside and outside the presumed cardholder area

In addition, the following should be assessed for the National Switch– Afghanistan Payment System including SWIFT CSP and CPMI-IOSCO Cyber resilience guidance.

41. **PCI-DSS Compliant:**

a. Network diagrams
b. Host configurations and standards
c. System configurations
d. System architecture
e. Policies and procedures
f. Technical standards
g. Encryption standards
h. Previous test and scan results

42. **To carry out a PCI-DSS assessment and provide plan to bridge the gaps**

To validate their compliance by either: 1) undergoing a PCI DSS assessment on their own and providing evidence of compliance to their customers, or 2) including their services for review in each of their customers' PCI DSS assessments.

Ensuring that the assessment cover all services provided to or used by the merchant, and that all applicable requirements were found to be in place for the environment and systems in scope.

43. **PCI DSS Gap Analysis**

Ability to carry out a gap analysis and evaluate how to achieve the following:

a. Build and maintain a secure network
b. Protect cardholder data
c. Maintain a vulnerability management program
d. Implement strong access control measures
e. Regularly monitor and test networks
f. Maintain an information security policy

44. **Controls Validation**

Ability to validate that controls in place are consistent with those required by the PCI DSS. Suppliermust be able to check to make sure that the controls are implemented as designed and documented, not merely that they exist. This phase includes technical testing, observation, review of configurations, etc. We may also review previous testing conducted, such as penetration tests, quarterly scans, wireless testing and any other technical testing you have performed.

This will be the ability to deploy industry best practices for vulnerability management—such as the OWASP Top 10, SANS2 CWE Top 25, and CERT3 Secure Coding—should be applied by e-commerce application/web developers. Merchants that purchase e-commerce applications should confirm that the application is validated according to PA-DSS. Merchants that develop their own e-commerce solutions should refer to PA-DSS as a best practice and/or confirm that the developer has knowledge of (and applies) strict and secure application coding/development practices.

Deliverables for Phase 1:

The vendor is required to complete all the activities in phase one and submit the report of accomplishment along with their findings and recommendations to DAB Project Manager.

Phase Two:

In the second phase, which will take time, as implementation of ATS and New CBS,willbe completed after some time, when the two applications implemented and become live then the security assessment vendor is required to complete their assessment as per the following details.

1. Complete Assessment of ATS (CSD, RTGS, ACH) after its implementation
2. Complete Assessment of New CBS after its implementation
3. Review and Evaluate that the three triad,securities Confidentiality, integrity and Availability (CIA) were deploy to the all above systems.

Vulnerability Assessment and Penetration Testing

1) **Gray Box Penetration Testing**
2) Active Assessment and Penetration Testing
3) External Assessment and Penetration Testing
4) Host-Based Assessment and Penetration Testing
5) Application Assessments and Penetration Testing
6) Passive Assessment and Penetration Testing
7) Internal Assessment and Penetration Testing
8) Network Assessment and Penetration Testing
9) Wireless Network Assessments and Penetration Testing
10) Examine and evaluate Physical Security
11) Footprinting and Reconnaissance
12) Web Server Assessment and Penetration testing
13) Review Cryptography
14) Web Application Assessment and Penetration testing
15) DHCP and Domain Assessment and Penetration Testing
16) Review and checking Physical Network Security Design
17) Scan Beyond IDS and Firewall
18) Perform Banner Grabbing/OS Fingerprinting
19) Application Debug Scanning
20) Scanning Buffer Overflows
21) Scanning Operating System Flaws

Deliverables (Phase2):

The vendor is required to complete all the activities in phase two and submit the report of accomplishment along with their findings and recommendations to DAB project manager.

PCI REMOTE REMEDIATION RETAINER

The firm will have access to DAB PCI experts for a period of time for the delivery of the PCI engagement.

Guide in formal policies, procedures, standards and guidance in template form to cover PCI requirements.

The assignment shall be implemented consecutivelyas under:
(1) PCI Gap assessment and analysis report and remediation plan,
(2) PCI Remediation Support,
(3) PCI Certification and Report on Compliance

Location of Performance:

The overall IS/IT Assessment is to be carried out at the four locations noted below;

a. DAB Headquarters, IbniSina Watt, Kabul
b. The disaster recovery site situated at Ministry of Communication, Kabul
c. The disaster recovery site situated at the Internet City, Dubai.
d. The Afghanistan Payment System in the vicinity of Ansari Square (Chara-heeAnsari), Share-e-Naw, Kabul

Transfer of Knowledge:

The firm should do knowledge transfer to DAB IT department during the assessment of different phases of deliverables. DAB technical team will be with firm during the assessment and the firm is responsible to make them understand performing different assessments, penetration tests etc. which is in scope of this TOR.

SUPERVISION:

The entire project of consultancy services would be monitored and supervised by the DG IT of Da Afghanistan Bank in the capacity as Project Manager.

4. Reporting:

4.1 Inception Report: Inception Report to be submitted within first 15 days from the date of commencement of the Consultancy Contract. The purpose of inception report is to set out a clear strategy and ways forward for the implementation of the technical assessment and the technological field as well as to specify the various activities, actions and outputs for this particular assessment, it should also include the approach and the methodology for a detailed work plan. The firm is required to do a detail on site study and come with detail action plan for performing the assessment.

4.2 Periodical Reports: The consultant shall submit these reports as defined under deliverables for different areas of scope of work for Phase 1 and 2above.The Periodical Reports shall be submitted at the end of every two months from the date of commencement of the Contract. The first Periodical Report would also include detail assessment of DAB IT department current infrastructure and an assessment of APS. The Second Periodical Report would also include pre assessment for New CBS and ATS.

4.3 Final Report: The Consultant shall submit Final Report including Assessment Report, Risks and Risks Mitigation Report, Assessment and Gap Analysis, Vulnerability Assessment and Penetration – Internal &External, Control Validation, etc. asper Scope of Services at the completion of tenure of nine months, including implementation of ATS, assessment after ATS is implemented and become live. The Assessment Report shall include an Executive Summary, Findings and Recommendations which should include, but not limited to, System Vulnerabilities, Security Program Management of Information Technology Resources and Application Life Cycle Controls.Also including detailed recommendations on any specific changes in network architecture, need for additional security related hardware and software, personnel requirements and additional training needs for DAB staff and including security architect to perform threat modelling/risk assessment and consolidate all the findings according to priority/impact and recommend data security controls based on assessment. Maybe the national switch security and VoIP security positions can be combined

Language:

All Reports need be submitted to theClient'sProject Manager in English.

5. The following facilities will be provided by the Client to consultant firm:

Suitable office space shall be provided to the Consultant Firm, equipped with Internet. The client shall facilitate and schedule meetings necessary for the Consultant Firm to carry out the assignment.

6. Team Composition and Qualification requirement for Key Experts:

S. No.	Key Expert Position	Number of Personnel	Estimated Person-Month
1	Position K 1: **Network Security Specialist**	1	2
2	Position K 2: **Application Security professional**	1	1.5
3	Position K 3: **Enterprise system professional**	1	2
4	Position K 4: **Data Centre Management and Data Centre Security Design professional**	1	1
5	Position K 5: **Database Security Specialist**	1	1.5
6	Position K 6: **Voice (VoIP) Security Specialist**	1	0.5
7	Position K 7:**National Switch Security Specialist**	1	0.5
	Total estimated Key Experts time inputs		9person months

Educational and certification requirements of Key Experts are shown in the Table below:

#	Key Staff	Minimum Qualifications/Certification requirements	Job Description (Minimum Task)
1	**Network Security Specialist**	Minimum Qualification: Bachelor Degree in Computer Science Minimum Certifications: CCIE Security, CISA, CISSP,CRISC,OWASP, CDCM, CDCDP	✓ Checking and evaluation of Cisco Switch configuration Packet Analysis ✓ Signal Capture ✓ Network Traffic Extraction ✓ Signal Transmission Network Protocol Analysis ✓ Network Protocol Traffic Capture ✓ Network Protocol Fuzzing ✓ Network Protocol Exploitation ✓ Inbound and outbound Firewall Penetration testing ✓ Physical checking the Network Equipment's ✓ Network Failover system ✓ Network Traffic Analyzing ✓ Evaluate Wireless Security ✓ Evaluate Network Vulnerability including DR Sites

2	**Application Security professional**	Minimum Qualification: Bachelor Degree in Computer Science Minimum Certifications: PHP, ASP.Net, C Security Certificates, CISA, CISSP,CRISC,OWASP, CDCM, CDCDP	Application Mapping ✓ Application Platform fingerprinting ✓ Functional analysis ✓ Process flow modelling ✓ Request/Response mapping Application Discovery ✓ Configuration management testing ✓ Authentication testing ✓ Session management testing ✓ Authorization testing ✓ Denial of Service Application Exploitation ✓ Identity attack avenues ✓ Vulnerability exploitation ✓ Post exploitation ✓ SQL injection ✓ Server port Scanning ✓ Cross site (XSS) web scanning ✓ Web site code scanning User Management ✓ Users management ✓ Authentication and Encryptions

3	**Enterprise system professional**	Minimum Qualification: Bachelor Degree in Computer Science Minimum Certifications: CCIE, MCSA, MCSA Security, CISA, CISSP,CRISC,OWASP, CDCM, CDCDP	Server OS penetration ✓ DNS interrogation ✓ Port Scanning ✓ Service Fingerprinting ✓ SNMP Enumeration ✓ Packet Sniffing Vulnerability Analysis ✓ Unauthenticated vulnerability scanning ✓ Authenticated vulnerability scanning ✓ Packet capture analysis ✓ Vulnerability validation Server OS Exploitation ✓ Identify attack avenues ✓ Vulnerability exploitation ✓ Post exploitation ✓ Evaluate server's vulnerability ✓ Evaluate active directory vulnerability exploitation ✓ DHCP scanning and penetration test and MAC DoS attack testing

4	**Data Centre Management and Data Centre Security Design professional**	Minimum Qualification: Bachelor Degree in Computer Science Minimum Certifications: CCIE and DATA Centre Required Security Certificates, CISA, CISSP,CRISC,OWASP, CDCM, CDCDP	Mechanic ✓ Cooling Systems ✓ Power Systems ✓ Fire systems ✓ Alarm Systems IT infrastructure ✓ Storage and network environments ✓ Cabling systems Security ✓ Best practice for standard data center security ✓ Access control ✓ Mantrap door systems Building ✓ Review building aria Asset Management ✓ Appreciate importance of assets management ✓ Develop an effective asset management strategy ✓ Asset management control
5	**Database Security Specialist**	Minimum Qualification: Bachelor Degree in Computer Science Minimum Certifications: Oracle MS SQL My SQL Securitycertificate, CISA, CISSP,CRISC,OWASP, CDCM, CDCDP	Outside in and inside out scan of all database ✓ Security strength ✓ Database vulnerabilities ✓ Fix security holes and misconfigurations ✓ Roles and responsibilities functionality to segregate users ✓ Backup procedure and data encryptions ✓ Perform database auditing and intrusion detection ✓ Authentication ✓ Server and database roles ✓ Authorization and permissions ✓ Code and data encryption

			✓ Securing tools and high availability ✓ Auditing policy
6	**Voice (VoIP) Security Specialist**	Minimum Qualification: Bachelor Degree in Computer Science CCIE Voice, CISA, CISSP,CRISC,OWASP, CDCM, CDCDP	✓ VoIP Policies ✓ Data classification policies and management ✓ Deployment or upgrade processes, ✓ Strategy and implementation control Technical ✓ Technical architecture(s) , including security systems, ✓ Backup and recovery ✓ Data retention and destruction policy ✓ Baseline configurations of deployed hardware and software ✓ Issues related to Centralized VoIP servers ✓ Issues related to failover VoIP
7	**National Switch Security Specialist**	Minimum Qualification: Bachelor Degree in Computer Science Minimum Certifications: CCIE Security Security necessary certificates, CISA, CISSP,CRISC,OWASP, CDCM, CDCDP	✓ APS Network Security assessment and penetration test ✓ APS application Security assessment ✓ APS hardware security assessment ✓ APS database security assessment ✓ APS PCI DSS assessment according in the scope of services of this document Performing the PCI DSS Assessment ✓ Being on-site for the duration of the PCI DSS Assessment ✓ Reviewing the work product that supports the PCI DSS Assessment

			procedures ✓ Ensuring adherence to the then-current PCI DSS ✓ Validating the scope of the PCI DSS Assessment ✓ Selecting systems and system components where sampling is employed ✓ Evaluating compensating controls ✓ Producing the final Report on Compliance (ROC)

All key experts should have the following qualifications and experience in addition to the above.

- Proven experience of similar project
- Minimum ten years' experience in Security Assessment
- Demonstrated required technical certified security skills
- Similar experience in developing countries desirable
- The following minimum security certified skills are required by the consultants doing the assessment
  - Application Security Assessment skill
  - Data Loss Prevention Technical Assessment skill
  - HIPAA Security and Compliance Assessment skill
  - Cyber Security Risk Assessment skill
  - Security Policy Development skill
  - PCI DSS Gap Analysis and Compliance Assessment skill
  - Security Training skill
  - Vulnerability Assessment skill
  - Penetration Testing skill
  - Phishing Simulation Risk Assessment skill
  - All the tools which are using for the said assessment should be international accepted standard tools and should be mentioned

8. **Duration:**

The Consultancy Services for theSecurity Assessment of DAB and APS IT Infrastructure as per Scope of Servicesis required to be accomplished within **Six months** from the date of signing of the Contractand The ATS and New CBS security assessment will be done in **three more** months

9. Payment Terms:

i. 15 % of the Contract Value shall be invoiced and payment released after submission and acceptance of the Inception Report

ii. 20 % of the Contract Value shall be invoiced and payment released after submission and acceptance of the 1st PhaseReport, eliciting accomplishment of Phase 1 Tasks.

iii. 20 % of the Contract Value shall be invoiced and payment released after submission and acceptance of the 2nd Phase Report, eliciting accomplishment of Phase 2 Tasks.

iv. The remaining balance 45 % of the Contract Value shall be invoiced and payment released after submission and acceptance of the Final Report.

10. Confidentiality:

The Consultant shall maintain complete confidentiality and shall not share any data/information gathered during the accomplishment of the assignment, with any other person/s/agencies without prior permission of the Client Da Afghanistan Bank.

11. Applicable law:

The prevailing laws of Afghanistan.