

TERMS OF REFERENCE

RECRUITMENT OF CYBERSECURITY CONSULTANT FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) TOWARD ISO 27001:2022 CERTIFICATION ECOWAS Bank for Investment and Development (EBID)

1. BACKGROUND AND CONTEXT

1.1. About ECOWAS Bank for Investment and Development (EBID)

The ECOWAS Bank for Investment and Development (EBID) is a specialized financial institution of the Economic Community of West African States (ECOWAS), headquartered in Lomé, Togo. Established to promote economic development and regional integration, EBID provides financing for development projects across the fifteen ECOWAS member states, supporting both public and private sector initiatives in key areas including infrastructure, agriculture, industry, and energy.

As a regional development finance institution, EBID operates in a complex and dynamic ICT environment that supports critical financial transactions, data management, stakeholder communications, and operational systems spanning multiple jurisdictions within the ECOWAS region.

1.2. Strategic Context and Rationale

In alignment with its IT Master Plan (2025-2027) and commitment to cybersecurity excellence, EBID is pursuing ISO 27001:2022 certification to establish a robust Information Security Management System (ISMS). This certification will demonstrate EBID's commitment to protecting sensitive financial data, maintaining stakeholder confidence, ensuring regulatory compliance, and adopting international best practices for information security.

The increasing sophistication of cyber threats targeting financial institutions, particularly in the banking and development finance sectors, necessitates proactive security measures. Vulnerability Assessment and Penetration Testing (VAPT) is a critical component of ISO 27001 compliance, specifically supporting Clauses A.8.8 (Technical Vulnerability Management) and A.12.6 (Management of Technical Vulnerabilities) of ISO 27001:2022.

1.3. Purpose of Assignment

EBID seeks to engage a qualified and experienced ICT Cybersecurity Consultant to conduct a comprehensive Vulnerability Assessment and Penetration Testing (VAPT) across its entire ICT infrastructure, applications, networks, and systems. The assessment will identify security vulnerabilities, evaluate the effectiveness of existing security controls, and provide actionable recommendations to strengthen EBID's cybersecurity posture in preparation for ISO 27001:2022 certification.

2. OBJECTIVES OF THE ASSIGNMENT

The primary objectives of this consultancy are to:

1. Support EBID in identifying the scope of the ISMS certification.
2. Support EBID in developing a RACI matrix for steering the ISO 27001:2022 SMSI project.
3. Conduct a comprehensive vulnerability assessment of EBID's ICT infrastructure, including networks, servers, databases, applications, endpoints, and cloud environments.
4. Perform penetration testing using industry-standard methodologies to simulate real-world cyberattacks and identify exploitable vulnerabilities.
5. Assess the security posture of EBID's core systems, financial applications, and critical business systems.
6. Evaluate compliance with ISO 27001:2022 requirements, particularly technical vulnerability management controls (Annex A.8.8, A.12.6, A.14.2).
7. Identify security gaps, misconfigurations, and weaknesses that could compromise the confidentiality, integrity, and availability of EBID's information assets.
8. Provide risk-based prioritization of identified vulnerabilities based on severity, exploitability, and business impact.
9. Deliver comprehensive technical and executive reports with detailed findings, risk ratings, and remediation recommendations.
10. Support EBID's management and technical teams with knowledge transfer and remediation guidance.
11. Conduct a post-remediation validation assessment to verify the effectiveness of implemented security controls.

12. Provide recommendations aligned with ISO 27001:2022 certification requirements and financial sector cybersecurity best practices.

3. SCOPE OF WORK

3.1. Assessment Coverage

The VAPT engagement shall comprehensively cover the following areas of EBID's ICT environment:

3.1.1. Network Infrastructure Assessment

- External network perimeter (e.g., firewalls, routers, switches, intrusion detection/prevention systems, etc.).
- Internal network segmentation and access controls.
- Virtual Private Networks (VPNs) and remote access solutions.
- Wireless networks (e.g., Wi-Fi security, guest networks, access point configurations, etc).
- Network monitoring and logging systems.
- Inter-branch connectivity and MPLS/WAN connections.
- Data center network architecture.
- Network security devices and configurations.

3.1.2. Server and Operating System Assessment

- Windows Server environments (e.g., Active Directory, Domain Controllers, File Servers, etc.).
- Linux/Unix server environments.
- Database servers (e.g., SQL Server, Oracle, MySQL, PostgreSQL, etc.).
- Application servers and middleware platforms.
- Virtualization infrastructure (e.g., VMware, Hyper-V, or equivalent).
- Backup and disaster recovery systems.
- Email and collaboration servers (e.g., Exchange, Office 365, etc.).
- Operating system hardening and patch management assessment.

3.1.3. Application Security Assessment

- Core systems and related modules.
- Internet and mobile-based applications.
- Payment processing and SWIFT systems.
- Financial management and accounting applications.
- Human resources and payroll systems.
- Document management and workflow systems.
- Customer relationship management (CRM) systems.
- Web portals and public-facing websites.
- APIs and web services (e.g., REST, SOAP, GraphQL).
- Custom-developed and third-party applications.

3.1.4. Cloud and Third-Party Services Assessment

- Cloud infrastructure (e.g., IaaS, PaaS, SaaS) configurations.
- Cloud storage security (data encryption, access controls).
- Identity and Access Management (IAM) configurations.
- Third-party integrations and vendor connections.
- Cloud service provider security configurations (e.g., Microsoft 365, Azure AD, ITSM SysAid, etc).

3.1.5. Endpoint and User Environment Assessment

- Workstation and laptop security configurations.
- Endpoint Protection Systems (antivirus, EDR solutions).
- Mobile device management (MDM) and mobile security.
- Privileged access management and administrative accounts.
- User authentication mechanisms and password policies.
- Multi-factor authentication (MFA) implementations.

3.1.6. Physical and Social Engineering Assessment

- Physical security controls and access management.
- Social engineering susceptibility testing (phishing simulations).
- Security awareness and user behaviour assessment.

- Insider threat vulnerability evaluation.

3.2. Testing Methodologies and Standards

The consultant shall employ internationally recognized methodologies and standards, including but not limited to:

- Open Web Application Security Project (OWASP) Top 10 and Testing Guide.
- OWASP Application Security Verification Standard (ASVS).
- Open-Source Security Testing Methodology Manual (OSSTMM).
- Penetration Testing Execution Standard (PTES).
- NIST SP 800-115 Technical Guide to Information Security Testing and Assessment.
- ISO 27001:2022 Annex A controls, particularly A.8.8, A.12.6, A.14.2.
- SANS Institute penetration testing methodologies.
- Common Vulnerability Scoring System (CVSS) v3.1 or later for risk rating.

3.3. Types of Testing

3.3.1. Vulnerability Assessment

- Verify the internal governance framework for vulnerability management.
- Automated vulnerability scanning using industry-standard tools.
- Manual verification and validation of identified vulnerabilities to eliminate false positives.
- Configuration review and security baseline assessment.
- Compliance checking against security frameworks and best practices.
- Missing patch and security update identification.
- Weak configuration and default credential detection.

3.3.2. Penetration Testing

The consultant shall conduct penetration testing using the following approaches:

3.3.2.1. External Penetration Testing (Black-Box)

- Simulating an external attacker with no prior knowledge of systems.
- Testing internet-facing assets, web applications, and external services.
- Attempting to breach perimeter defences and gain unauthorized access.

- Exploitation of identified vulnerabilities to demonstrate real-world impact.

3.3.2.2. Internal Penetration Testing (Gray-Box)

- Simulating a malicious insider or a compromised internal user.
- Testing internal network segmentation and lateral movement controls.
- Privilege escalation testing.
- Internal application and service exploitation.

3.3.2.3. Web Application Penetration Testing

- SQL injection, Cross-Site Scripting (XSS), and Cross-Site Request Forgery (CSRF) testing.
- Authentication and session management testing.
- Business logic vulnerability assessment.
- API security testing (e.g., authentication, authorization, input validation, etc.).
- Insecure direct object references and access control testing.

3.3.2.4. Wireless Network Penetration Testing

- Wi-Fi encryption and authentication security.
- Rogue access point detection.
- Wireless network segmentation assessment.
- Man-in-the-middle attack simulation.

3.3.2.5. Social Engineering Testing

- Targeted phishing campaign simulation.
- Vishing (voice phishing) assessment (if applicable).
- Physical security bypass testing (with proper authorization).

3.4. Threat-Led Penetration Testing (TLPT)

3.4.1. Purpose

In addition to conventional Vulnerability Assessment and Penetration Testing (VAPT), the Consultant shall conduct a Threat-Led Penetration Testing (TLPT) exercise designed to

simulate realistic, intelligence-driven cyberattack scenarios against EBID's critical business services and supporting infrastructure.

The TLPT engagement shall assess EBID's capability to:

- Prevent sophisticated cyberattacks.
- Detect malicious activity promptly.
- Respond effectively to security incidents.
- Contain and recover from advanced threat scenarios.
- Strengthen resilience in alignment with ISO 27001:2022 operational and incident management controls.

3.4.2. Scope of TLPT

The TLPT shall target EBID's identified Critical Business Services (CBS) and high-value assets, including but not limited to:

- Core systems.
- Payment systems and SWIFT infrastructure.
- Internet and mobile banking platforms.
- Identity and Access Management (IAM) systems.
- Privileged Access Management (PAM) environments.
- Network infrastructure and security monitoring systems.
- Cloud-hosted financial services.
- Active Directory and domain services.

The Consultant shall design threat scenarios based on relevant financial-sector threat intelligence, including but not limited to:

- Advanced Persistent Threat (APT) campaigns.
- Ransomware attack scenarios.
- Credential theft and account takeover.
- Lateral movement within internal networks.
- Supply chain compromise.
- Insider threat simulation.
- Targeted phishing campaigns and social engineering.

3.4.3. Methodological Framework

The TLPT shall be conducted using internationally recognized adversary simulation methodologies, including:

- MITRE ATT&CK framework mapping.
- Intelligence-led attack scenario development.
- Kill Chain modelling.
- NIST SP 800-61 Incident Handling Guidance.
- ISO 27001:2022 Annex A controls relating to monitoring, logging, and incident management.

The TLPT shall be structured into the following phases:

3.4.3.1. Phase 1 – Threat Intelligence and Scenario Development

- Collection of sector-specific threat intelligence.
- Identification of relevant threat actors.
- Mapping of tactics, techniques, and procedures (TTPs).
- Development of realistic attack scenarios.
- Definition of Rules of Engagement (RoE).
- Identification of critical assets (“crown jewels”).

3.4.3.2. Phase 2 – Red Team Exercise (Adversary Simulation)

- Controlled and covert attack execution (as authorized).
- Initial access attempts.
- Privilege escalation.
- Lateral movement.
- Persistence establishment.
- Command and control simulation.
- Controlled data exfiltration simulation.
- Defence evasion techniques.

3.4.3.3. Phase 3 - Detection and Response Assessment

- Evaluation of monitoring and alerting capabilities.
- Incident response timeline analysis.
- Measurement of Mean Time to Detect (MTTD).

- Measurement of Mean Time to Respond (MTTR).

3.4.3.4. Phase 4 - Control Effectiveness and Resilience Evaluation

- Evaluation of preventive, detective, and corrective controls.
- Review of logging and forensic readiness.
- Assessment of recovery capability.
- Identification of systemic weaknesses.

All testing activities shall strictly adhere to the agreed Rules of Engagement and shall not cause uncontrolled disruption to production systems.

3.4.4. Rules of Engagement and Safety Controls

Prior to commencement, the Consultant shall:

- Obtain formal written authorization from EBID.
- Define detailed Rules of Engagement.
- Establish escalation and emergency stop procedures.
- Identify protected systems and operational constraints.
- Ensure non-destructive payload execution unless explicitly approved.
- Maintain secure logging of all testing activities.
- Denial-of-Service (DoS) attacks or destructive techniques shall be conducted outside the production environment.

3.5. Exclusions and Constraints

- Testing shall be conducted during agreed-upon timeframes to minimize disruption to business operations.
- Load testing may be discussed separately if required.
- Testing of production systems shall follow agreed-upon rules of engagement and safety protocols.
- Any destructive testing shall require explicit written approval from EBID's ICT management.
- Third-party systems outside EBID's direct control may be excluded unless proper authorization is obtained.

4. DELIVERABLES AND REPORTING REQUIREMENTS

4.1. Inception Report

Timeline: Within 5 working days of contract commencement.

Contents:

- Detailed work plan and testing schedule.
- Methodology and approach documentation.
- Scope confirmation and asset inventory verification.
- Tools and techniques to be employed.
- Risk mitigation strategies for testing activities.
- Communication and escalation protocols.
- Testing team composition and qualifications.

4.2. Progress Reports

Timeline: Weekly during the active testing phase.

Contents:

- Summary of activities completed.
- Preliminary findings and critical vulnerabilities discovered.
- Challenges encountered and mitigation measures.
- Upcoming activities and schedule adherence.

4.3. Draft VAPT Technical Report

Timeline: Within 15 working days of testing completion.

Contents:

- Executive summary with overall security posture assessment.
- Detailed methodology and testing scope.
- Comprehensive vulnerability findings with technical details.
- Risk classification using CVSS scores and business impact analysis.
- Evidence documentation (e.g., screenshots, logs, proof-of-concept, etc.).
- Attack chain analysis and exploitation scenarios.
- Detailed remediation recommendations with prioritization.
- Compliance gap analysis against ISO 27001:2022 requirements.
- Security control effectiveness evaluation.

- Technical appendices and supporting documentation.

4.4. Executive Summary Report

Timeline: Concurrent with Draft Technical Report.

Contents:

- High-level overview of security assessment findings.
- Risk summary and key vulnerabilities requiring immediate attention.
- Business impact analysis of identified risks.
- Issue resolution and remediation recommendations.
- Strategic recommendations for management.
- Compliance status toward ISO 27001:2022 certification.
- Visual representations (e.g., graphs, charts, heat maps, etc.).
- Non-technical language suitable for the board and senior management.

4.5. Final VAPT Report

Timeline: Within 10 working days of receiving feedback on the draft report.

Contents:

- Incorporation of EBID's feedback and clarifications.
- Refined findings and recommendations.
- Updated risk assessments based on additional information.
- Comprehensive final technical and executive reports.

4.6. Remediation Validation Report

Timeline: Within 10 working days of completing post-remediation testing (typically 60-90 days after final report delivery).

Contents:

- Verification of implemented remediation measures.
- Re-testing of previously identified vulnerabilities.
- Assessment of residual risks.
- Confirmation of security control effectiveness.
- Updated compliance status.
- Recommendations for continuous improvement.

4.7. Threat-Led Penetration Testing (TLPT) Deliverables

The following deliverables shall be produced as part of the TLPT engagement and shall complement the standard VAPT deliverables defined in this Chapter.

4.7.1. TLPT Threat Intelligence and Scenario Design Report

Timeline: Within 10 working days following completion of the Threat Intelligence and Scenario Development Phase.

Contents:

- Threat landscape overview relevant to development finance institutions and regional banking environments.
- Identification of threat actors, capabilities, and motivations.
- Mapping of identified tactics, techniques, and procedures (TTPs) to the MITRE ATT&CK framework.
- Defined attack scenarios and supporting rationale.
- Risk exposure hypothesis for EBID's critical business services.
- Identification and prioritization of high-value assets ("crown jewels").

4.7.2. TLPT Red Team Technical Report

Timeline: Within 15 working days after completion of the Red Team exercise.

Contents:

- Executive summary of attack outcomes.
- Detailed attack narrative structured using Kill Chain analysis.
- Initial access vectors exploited.
- Privilege escalation techniques and lateral movement paths.
- Persistence mechanisms identified.
- Simulated data exfiltration results.
- Defence evasion and control bypass techniques.
- Technical evidence (screenshots, logs, proof-of-concept artifacts).
- Risk severity assessment aligned with business impact analysis.
- Mapping of exploited techniques to ISO 27001:2022 relevant controls.

4.7.3. Detection and Response Effectiveness Report

Timeline: Concurrent with the TLPT Red Team Technical Report.

Contents:

- Alert generation and quality analysis.
- Detection capability gaps.
- Incident escalation and communication review.
- Measurement of Mean Time to Detect (MTTD).
- Measurement of Mean Time to Respond (MTTR).
- Assessment of monitoring and logging effectiveness.
- Recommendations for improvements in detection engineering and monitoring.
- Incident response maturity observations.

4.7.4. TLPT Executive Briefing

Timeline: Delivered concurrently with the Final TLPT Reports.

Format: Board-level presentation and executive summary document.

Contents:

- Overall cyber resilience and maturity rating.
- Business impact analysis of simulated attack scenarios.
- Identification of critical systemic weaknesses.
- Strategic cybersecurity maturity gaps.
- Investment prioritization recommendations.
- Alignment analysis with ISO 27001:2022 requirements and Annex A controls.
- High-level remediation priorities and governance considerations.

The presentation shall be suitable for senior management and Board-level stakeholders.

4.7.5. Remediation and Improvement Roadmap

Timeline: Delivered with the Final TLPT Technical Report.

Contents:

- Prioritized remediation plan (e.g., short-, medium-, and long-term actions).
- Defensive architecture improvement recommendations.
- Monitoring and logging enhancement plan.
- Incident response maturity roadmap.

- Governance and policy enhancement recommendations.
- Continuous improvement alignment with ISO 27001:2022.

4.7.6. Post-Remediation TLPT Validation Report

Timeline: Within 10 working days following completion of post-remediation validation testing (typically 60-90 days after submission of the Final TLPT Report).

Contents:

- Re-testing of previously exploited attack paths.
- Verification of improved detection and response capability.
- Assessment of residual risk exposure.
- Updated resilience rating.
- Confirmation of control effectiveness.
- Recommendations for further improvement, if applicable.

4.8. Knowledge Transfer and Presentation

Timeline: Upon delivery of the final report and validation report.

Contents:

- Detailed presentation of findings to EBID's technical and management teams.
- Interactive Q&A sessions.
- Remediation guidance and best practices workshop.
- Security awareness recommendations.
- Documentation of lessons learned.

5. CONSULTANT QUALIFICATIONS AND REQUIREMENTS

5.1. Mandatory Qualifications

The consulting firm or individual consultant must demonstrate the following qualifications:

5.1.1. Organizational Requirements

- Registered and legally operating in their country of operation.
- Minimum 7 years of experience providing cybersecurity and penetration testing and Threat-Led Penetration Testing (TLPT) services.
- Proven track record of conducting VAPT for financial institutions, banks, or development finance institutions.

- Demonstrated involvement in at least four (4) medium to large financial system environments, including security architecture, assurance, or protection of mission-critical platforms.
- Certified in ISO27001 (Information Security Management) and ISO22301 (Business Continuity Management).
- Experience supporting ISO 27001 certification projects.
- Valid professional liability insurance covering cybersecurity consulting services.
- Adherence to professional ethical standards and codes of conduct.

5.1.2. Technical Team Qualifications

The proposed technical team must include professionals with the following certifications (minimum requirements for each profile):

5.1.2.1. Lead Penetration Tester/Security Consultant

- Offensive Security Certified Professional (OSCP), or
- Certified Ethical Hacker (CEH) - EC-Council, or
- GIAC Penetration Tester (GPEN), or
- Certified Penetration Testing Engineer (CPTE).
- Minimum 5 years of hands-on penetration testing experience.

5.1.2.2. ISO 27001 Specialist:

- ISO 27001 Lead Auditor or Lead Implementer certification.
- Minimum 5 years of experience in ISO 27001 implementation and auditing.
- Experience in the financial sector compliance.

5.1.2.3. Web Application Security Specialist:

- Offensive Security Web Expert (OSWE), or
- GIAC Web Application Penetration Tester (GWAPT), or
- Certified Web Application Security Tester (equivalent).
- Experience in banking application security testing

5.1.2.4. Network Security Specialist:

- Cisco Certified Network Professional (CCNP) Security, or

- GIAC Certified Intrusion Analyst (GCIA), or
- CompTIA Security+ with network security specialization.
- Minimum 4 years of network security experience.

5.1.3. Desirable Additional Certifications

- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM).
- GIAC Security Essentials (GSEC).
- Certified Cloud Security Professional (CCSP).
- Payment Card Industry Professional (PCIP).
- Offensive Security Certified Expert (OSCE).
- Certified Information Systems Auditor (CISA).

5.2. Experience Requirements

- Minimum of 5 successfully completed VAPT and TLPT projects for financial institutions, banks, or similar organizations.
- At least 3 completed ISO 27001 certification support projects.
- Demonstrated experience in the African or West African banking sector (highly desirable).
- Experience with core banking systems security assessment (highly desirable).
- Familiarity with regional regulatory requirements (BCEAO, ECOWAS central bank regulations, etc.).
- Experience conducting VAPT in multilingual and multicultural environments.

5.3. Technical Capabilities

- Proficiency in industry-standard vulnerability assessment, penetration testing, and TLPT tools.
- Expertise in both automated scanning and manual testing techniques.
- Ability to develop custom exploits and testing scripts.
- Experience with secure coding practices and application security.
- Knowledge of financial sector cybersecurity frameworks and regulations.
- Understanding of VM and cloud security (e.g., AWS, Azure, Google Cloud, etc.).

- Capability to conduct assessments with minimal business disruption.

5.4. Language Requirements

- Fluency in English (mandatory).
- Fluency in French (mandatory for ECOWAS/EBID context).
- All deliverables must be provided in both English and French.

6. DURATION AND TIMELINE

6.1. Contract Duration

The total duration of the consultancy shall be approximately **100 calendar days** from the date of contract signing, with the following indicative timeline:

Phase	Activity	Duration
Phase 1	• Contract Signing and Mobilization	Days 1-5
Phase 2	• Inception Meeting and Planning	Days 5-10
Phase 3	• Vulnerability Assessment	Days 10-25
Phase 4	• Penetration Testing (External & Internal) & TLPT	Days 25-60
Phase 5	• Analysis and Report Preparation	Days 60-75
Phase 6	• Draft Report Submission and Review	Days 75-85
Phase 7	• Final Report Submission	Days 85-90
Phase 8	• Presentation and Knowledge Transfer	Days 90-100
Phase 9	• Post-Remediation Validation (after 60-90 days)	As scheduled

Table 1: Indicative Project Timeline.

6.2. Work Location

- On-site presence at EBID Headquarters in Lomé, Togo, is required for:
 - ∞ Inception meetings and project kick-off.
 - ∞ Internal network and physical security testing.
 - ∞ Final presentation and knowledge transfer sessions.
- Remote work is acceptable for:
 - ∞ External penetration testing.

- ∞ Report preparation and analysis.
- ∞ Progress reporting and coordination.
- Estimated on-site presence: 15-20 working days distributed across project phases.

7. EBID'S RESPONSIBILITIES

EBID shall provide the following support to facilitate successful project execution:

- Designation of a project focal point and technical liaison officer.
- Access to necessary ICT infrastructure, systems, and documentation.
- Provision of testing credentials and access rights as required.
- Network diagrams, system architecture documentation, and asset inventory.
- Share the list of the VLAN.
- Coordination with relevant departments and system administrators.
- Office workspace and meeting facilities during on-site visits.
- Timely review and feedback on deliverables.
- Coordination with third-party vendors where required.
- Authorization letters and legal documentation for penetration testing activities.

8. CONFIDENTIALITY AND DATA PROTECTION

- The consultant shall sign a comprehensive Non-Disclosure Agreement (NDA) prior to the commencement of the contract.
- All information, data, and findings shall be treated as strictly confidential.
- The consultant shall not disclose any EBID information to third parties without explicit written consent.
- All testing data, reports, and materials shall be securely destroyed or returned to EBID upon project completion.
- The consultant shall comply with applicable data protection and privacy regulations.
- EBID retains all intellectual property rights to deliverables and findings.
- The consultant shall implement appropriate security measures to protect EBID's data during the engagement.
- Secure storage protocols during the engagement.
- Certified data destruction procedures at the end of the mission.
- Restrictions on the use of cloud tools (to prevent potential data leakage).

9. EVALUATION CRITERIA

Proposals shall be evaluated using a **Quality and Cost-Based Selection (QCBS)** methodology with the following distribution:

- Technical Quality: 70%
- Financial Proposal: 30%

9.1. Technical Evaluation Criteria (70 points)

Criteria	Maximum Points
Consultant's Qualifications and Experience	20
Organizational profile and track record	(8)
Relevant certifications and accreditations	(7)
Financial sector experience	(5)
Proposed Methodology and Approach	25
Comprehensiveness of methodology	(10)
ISO 27001 alignment strategy	(8)
Risk mitigation and safety protocols	(7)
Technical Team Composition and Expertise	15
Team leader qualifications and experience	(6)
Team member certifications and expertise	(6)
ISO 27001 specialist qualifications	(3)
Understanding of Assignment and Work Plan	10
Scope understanding and coverage	(5)
Timeline realism and project management	(5)
TOTAL TECHNICAL SCORE	70
<ul style="list-style-type: none"> • NOTE: <ul style="list-style-type: none"> ○ <u>Minimum Technical Score:</u> 49 points (70% of Technical Score). 	

Table 2: Technical Evaluation Scoring Matrix.

9.2. Financial Evaluation (30 points)

Financial proposals shall be evaluated using the formula:

$$\text{Financial Score} = \left(\frac{\text{Lowest Evaluated Price}}{\text{Price of Proposal}} \right) \times 30$$

9.3. Final Combined Score

$$\text{Final Score} = \text{Technical Score} + \text{Financial Score.}$$

The consultant with the highest combined score shall be selected for contract negotiation.

10. SUBMISSION REQUIREMENTS

10.1. Technical Proposal

The technical proposal shall include:

1. Cover letter and executive summary.
2. Company profile and registration documents.
3. Detailed understanding of the assignment and objectives.
4. Proposed methodology and approach.
5. Detailed work plan and timeline.
6. Team composition with CVs and certifications.
7. Evidence of similar past assignments (minimum 5 reference projects).
8. Contact details for at least 3 professional references.
9. Tools and technologies to be employed.
10. Quality assurance and validation procedures.
11. Risk management and mitigation strategies.

10.2. Financial Proposal

The financial proposal shall be submitted separately and include:

1. Total lump-sum fee in USD (USD Dollars).
2. Detailed cost breakdown:
 - Professional fees by team member.
 - Travel and accommodation costs.
 - Tools and software licenses (if applicable).
 - Report production and documentation.
 - Post-remediation validation costs.
 - Any other anticipated expenses.

3. Payment schedule linked to deliverables.
4. Validity period of the proposal (minimum 90 days).
5. Tax and regulatory compliance information.

10.3. Supporting Documents

1. Business registration certificate.
2. Tax clearance certificate.
3. Professional liability insurance certificate.
4. Professional certifications (e.g., OSCP, CEH, ISO 27001 Lead Auditor, etc.).
5. Corporate profile and brochures.
6. Quality management system documentation (if applicable).
7. Anti-corruption and ethical conduct declarations.

11. SUBMISSION DETAILS

Submission Deadline:	May 28, 2026, at 10:00 AM GMT
Submission Method:	<ul style="list-style-type: none"> • Electronic submission via email and hard copy.
Electronic Submission:	<ul style="list-style-type: none"> • ichabimougnan@bidc-ebid.org/secretariatdasg@bidc-ebid.org
Hard Copy Submission:	<ul style="list-style-type: none"> • ECOWAS Bank for Investment and Development.
	<ul style="list-style-type: none"> • Services General Division.
	<ul style="list-style-type: none"> • 128 Boulevard du 13 Janvier.
	<ul style="list-style-type: none"> • BP 2704, Lomé, Togo.
Proposal Format:	<ul style="list-style-type: none"> • Technical Proposal (separate sealed envelope).
	<ul style="list-style-type: none"> • Financial Proposal (separate sealed envelope).
	<ul style="list-style-type: none"> • Both in English and French.
Clarification Requests:	<ul style="list-style-type: none"> • Submit by May 21, 2026.
	<ul style="list-style-type: none"> • Via email: ichabimougnan@bidc-ebid.org/secretariatdasg@bidc-ebid.org
Expected Contract Award:	<ul style="list-style-type: none"> • July 2026.

Project	• July 2026.
Commencement:	

Table 3: Submission Details.

12. PAYMENT TERMS LINKED TO DELIVERABLES

Payments shall be made in USD (United States Dollars) based on the following schedule:

Deliverable/Milestone	Percentage of Total Fee
Upon Contract Signing (Mobilization Advance)	50%
Submission and Approval of Inception Report	0%
Completion of Vulnerability Assessment and Penetration Testing	0%
Submission and Approval of Draft VAPT Report	0%
Submission and Approval of Final VAPT Report	30%
Completion of Presentation and Knowledge Transfer	0%
Completion of Post-Remediation Validation Report	20%
TOTAL	100%

Table 4: Payment Schedule.

All payments are subject to:

- Satisfactory completion and approval of deliverables.
- Submission of valid tax invoices.
- Compliance with contractual obligations.
- Deduction of applicable withholding taxes as per Togolese tax regulations.

13. GENERAL TERMS AND CONDITIONS

13.1 Compliance and Ethical Standards

- The consultant shall comply with EBID's procurement policies and procedures.
- Zero tolerance for fraud, corruption, and unethical practices.
- Adherence to professional codes of conduct and industry standards.
- Compliance with applicable laws and regulations in Togo and the ECOWAS region.

13.2 Conflict of Interest

- The consultant must declare any potential conflicts of interest.
- No participation in subsequent implementation or remediation work derived from this assessment (cooling-off period of 12 months).
- Independence and objectivity must be maintained throughout the engagement.

13.3 Intellectual Property

- All reports, findings, and deliverables become the exclusive property of EBID.
- EBID reserves the right to publish or share findings as deemed appropriate.
- The consultant may reference the project in their portfolio with prior written consent (without disclosing confidential information).

13.4 Insurance and Liability

- The consultant shall maintain adequate professional indemnity insurance.
- Minimum coverage of USD 50,000 for professional liability.
- The consultant is responsible for any damages caused by negligence or non-compliance with agreed protocols.

13.5 Contract Termination

EBID reserves the right to terminate the contract under the following circumstances:

- Breach of confidentiality or data protection obligations.
- Failure to deliver agreed-upon deliverables within specified timelines.
- Substandard quality of work as determined by EBID.
- Violation of ethical standards or professional conduct.
- Force majeure events beyond the control of either party.

14. CONTACT INFORMATION

For further information and clarifications regarding these Terms of Reference, please contact:

ECOWAS Bank for Investment and Development (EBID)

Services General Division Procurement and Contract Management Unit.

Address : 128 Boulevard du 13 Janvier BP 2704, Lomé, Togo.

Email : approvisionnement@bidc-ebid.org.

Website: www.bidc-ebid.org.

Attention: Chairman, Procurement Committee.

15. CONTENTS OF TECHNICAL AND FINANCIAL OFFER

THE TECHNICAL OFFER MUST NOT CONTAIN THE FINANCIAL INFORMATION, FAILING WHICH THE OFFER SHALL BE REJECTED.

A. THE FINANCIAL OFFER

The financial offer expressed in US Dollars , duty-free shall be broken down as follows :

- Fixed amount :

Honorarium (detail per expert).

- Reimbursable fees:

- o Subsistence allowance (accommodation and feeding) ;
- o Air tickets ;
- o Local transport ;
- o Miscellaneous expenses (communication, administration and preparation of reports, etc.).

The fees for all activities and input described in the technical proposal must be stated separately. It is assumed that the activities and input described in the technical proposal for which no cost is indicated are included in the costs for other activities and input. When the mission involves several stages, steps or activities, the cost of each of them must be clearly stated in the financial offer.

The original and the copy of the technical proposal must be enclosed in a stamped envelope clearly marked with the indication « **TECHNICAL PROPOSAL RECRUITMENT OF CYBERSECURITY CONSULTANT FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) TOWARD ISO 27001:2022 CERTIFICATION ECOWAS Bank for Investment and Development (EBID)**

», name and address of the Consultant, and an inscription « DO NOT OPEN BEFORE THE OPENING OF TECHNICAL PROPOSALS SESSION ».

Also, the original and the copy of the financial proposal must be enclosed in a stamped envelope clearly marked with the indication « **FINANCIAL PROPOSAL RECRUITMENT OF A**

RECRUITMENT OF CYBERSECURITY CONSULTANT FOR VULNERABILITY ASSESSMENT AND PENETRATION TESTING (VAPT) TOWARD ISO 27001:2022 CERTIFICATION

ECOWAS Bank for Investment and Development (EBID)

», name and address of the Consultant, and an inscription « NOT TO BE OPENED AT THE SAME TIME AS THE TECHNICAL PROPOSAL ».

These two stamped envelopes containing the technical proposal and the financial proposal shall be enclosed in a stamped envelope. This envelope shall bear the address of submission of the bids, an inscription as follows « DO NOT OPEN BEFORE THE OPENING OF TECHNICAL PROPOSALS SESSION ».

ALL FINANCIAL PROPOSALS NOT SUBMITTED IN A SEPARATE ENVELOPE BEARING THE INDICATIONS STATED HERE-ABOVE SHALL AUTOMATICALLY ENTAIL REJECTION OF THE BID.

The technical and the financial offers must respectively be submitted in two (2) copies of which one (1) original and one (1) copy marked as such. In case of difference, the original shall be considered. **In addition, the consultant must join a CD or a USB drive containing his technical and financial offers.**

All the pages of the proposal must be initialed by a duly mandated representative of the Consultant. The proposal from a consortium must be signed by all the members of the consortium, to ensure that this is legally binding on them or by a representative so empowered, who would have a power of attorney signed by all the authorized representatives of the consortium.

16. CRITERIA FOR EVALUATION OF BIDS

Evaluation of the bids which would be handled by a Committee shall be conducted in two stages. Firstly, the Committee shall assess the technical bids based on the following criteria and sub-criteria:

- a. General qualifications of the bidder for the mission: **10 points**;
- b. Compliance of the work plan and of the technical approach with the terms of reference (TOR) **30 points**;
- c. **Sub-criteria:** technical approach and methodology (20); a detailed work plan (10); Similar works (at least 4): **20 points**
- d. Qualifications and competence of key staff for the mission: **40 points**

Total : 100 points

Secondly, the financial proposals shall be analyzed. Only the financial offers from the bidders that would have obtained up to or more than 80 points shall be opened and undergo financial evaluation. The financial offers shall be assessed duty-free.

The lowest bid shall receive the maximum financial score (Sf) of 100 points. The financial score (Sf) of the other financial proposals shall be calculated using the following formula: **$Sf = 100 \times Fm/F$** , F being the financial amount of the proposal of which the score is being sought.

The proposals shall be classified based on the weighting of the technical and the financial scores. (The technical proposal shall be weighted 0.80 while the financial proposal shall be weighted 0.20).

The Consultant that would have obtained the highest score from a combination of technical and the financial score shall be invited for negotiations for the award of the contract.

The offers must remain valid for ninety (90) days with effect from the deadline for submission of bids, if eventually these are extended. During this period, the Consultant must maintain his initial proposal without change, including the key staff, the rates and total prices proposed.

17. DATE AND VENUE FOR SUBMISSION OF THE BIDS

Bids prepared in French or English languages must be submitted to the following address:

Secretariat of the Director of Administration and General Services
ECOWAS Bank for Investment and Development
128, Boulevard du 13 Janvier
B.P. 2704 Lomé – Togo
Tel : (228) 22 21 68 64

At the latest by **May 28, 2026 at 10.00 am**. The bids shall be opened ideally the same date by 10:30 am, if possible.

No bid must be sent by electronic mail. Bids received after the time and deadline shall not be assessed.

For all information relating to the present terms of reference, please send an email ichabimoungnan@bidc-ebid.org/secretariatdasg@bidc-ebid.org.

18. ANNEXES

Annex A: Asset Inventory Template

To be provided to the shortlisted consultants

Annex B: Network Architecture Diagrams

To be provided upon contract signing

Annex C: Non-Disclosure Agreement Template

To be signed prior to contract commencement

Annex D: ISO 27001:2022 Compliance Checklist

To be used for gap analysis

Annex E: Vulnerability Classification Matrix

Risk rating and prioritization framework.

Annex F: EBID ICT Security Policies

Relevant excerpts to be shared with the selected consultant.