SOUTHBANK INC.

IT Vendor Accreditation Policy

Document Revision History:

Version	Date	Author	Description of Changes

1. PURPOSE

The purpose of this IT Vendor Accreditation Policy is to establish a standardized and transparent process for evaluating, selecting, accrediting, and renewing partnerships with Information Technology (IT) vendors.

This policy ensures that all IT vendors meet the organization's technical, operational, financial, and compliance requirements to mitigate risks and achieve high performance standards.

The policy seeks to:

1. Ensure only competent and reliable vendors are engaged.
2. Protect the organization from technical, security, and operational failures.
3. Support strategic goals through partnerships with capable IT providers.
4. Promote fairness, transparency, and due diligence in the procurement process.

2. SCOPE

This policy applies to all external IT vendors, contractors, and service providers engaged by the organization for any of the following:

1. Software and system development
2. Infrastructure and hardware solutions
3. Cybersecurity products and services
4. IT consulting and professional services
5. Managed services and support
6. Cloud services and hosting
7. Network equipment and implementation
8. Others that are related to IT Operations

3. VENDOR ACCREDITATION REQUIREMENTS

3.1. BUSINESS INFORMATION

Vendors must submit complete documentation detailing:

1. Company profile and ownership structure (Sole Proprietorship, Partnership, or Corporation)
2. Business registration (SEC/DTI/CDA) and permits
3. Valid tax identification number (TIN) and BIR registration
4. Audited financial statements (latest 2 years)
5. Organization structure with key technical personnel and certifications (if any)

For item number 4 (AFS), a vendor may submit at a later time (not more than a year), provided that it is not yet available.

3.2. EXPERTISE OF THE FIELD

The vendor must demonstrate and provide proof of technical expertise in relevant areas, including but not limited to the following checklist – this will vary depending on the nature of engagement:

1. **Domain-specific experience:** (such as banking, telecom, retail, government).
2. **Industry-recognized certifications:** (such as ISO, ITIL, PCI DSS, AWS, Microsoft, Cisco)
3. **Specialized skills**: In either cybersecurity, cloud computing, systems integration, or software development, depending on the nature of the project or requirement.
4. **Availability of skilled support and project teams:** With relevant certifications, training, or similar implementation experience.
5. **Regulatory and compliance expertise**: Including familiarity with data privacy, financial regulations, and industry-specific compliance standards (e.g., GDPR, BSP regulations, AMLA).
6. **Proven track record of similar implementations**: With references or case studies demonstrating successful delivery in comparable environments.
7. **Innovation and adaptability**: Showing the ability to integrate emerging technologies (e.g., AI/ML, Regulators) into solutions when appropriate.
8. **Business continuity and disaster recovery expertise**: Including experience in resilience planning, backup solutions, and recovery testing.
9. **Security and risk management capabilities**: Including vulnerability assessment, penetration testing, and risk mitigation strategies.
10. **Vendor partnerships and ecosystem integration**: Demonstrating active collaborations with leading technology providers or industry alliances.
11. **Training and knowledge transfer programs**: Ensuring capability-building within the client's teams for sustainability beyond project delivery. This includes training modules, documentation, and service delivery execution.
12. **Scalability and performance optimization experience**: Ensuring solutions can handle growth, peak loads, and long-term business needs.

3.3. PROJECT HIGHLIGHTS AND DEPLOYMENT EXPERIENCE

Vendor must provide:

1. A list of successful past projects with deployment details, especially those in regulated industries or relevant industries, about the nature of the project. (such as banking, government, insurance etc.)
2. Case studies or summaries of at least 3 major deployments within the last 5 years
3. Client references or testimonials highlighting effectiveness, innovation, and post-deployment support
4. Projects showcasing large-scale rollouts, high availability systems, cybersecurity implementations, and compliance integrations

Preference will be given to vendors that:

1. Have handled projects with complexity similar to the organization's needs.
2. Have demonstrated pre- and post-implementation planning, support, and upgrade cycles.
3. Can show measurable outcomes from past projects (such as uptime, cost savings, efficiency gains)

4. ACCREDITATION PROCESS

1. **Application Submission:** Vendors must submit an accreditation form and all supporting documents.
2. **Evaluation:** Evaluation will be based on technical capability, experience, compliance, financial stability, and previous deployments.
3. **Due Diligence & Validation:** References and certifications will be validated. Site visits or interviews may be conducted if necessary.
4. **Approval:** IT Unit shall endorse the qualified IT Vendors to the IT Steering Committee, or EXECOM, for review and approval of vendors for accreditation.
5. **Accreditation Validity:** Accreditation is valid for two (2) years, subject to annual performance monitoring and re-evaluation.

5. PERFORMANCE MONITORING

Accredited vendors are subject to regular performance evaluations based on:

1. Delivery Requirements and Timelines
2. Quality of service
3. Security and compliance adherence
4. Communication and collaboration
5. Issue resolution and support
6. Poor performance or breach of agreement may lead to suspension or termination of accreditation.

To comply with this procedure, please refer to Annex 2: IT VENDOR PERFORMANCE ASSESSMENT.

6. Review and Updates

This policy shall be reviewed at least once every two (2) years or as necessary to ensure alignment with evolving technology, regulatory changes, and organizational needs.

Attachments:

Annex 1: IT VENDOR ACCREDITATION DOCUMENT

Annex 2: IT VENDOR PERFORMANCE ASSESSMENT

Annex 3: IT VENDOR PRE-ONBOARDING CHECKLIST

Annex 1: IT VENDOR ACCREDITATION DOCUMENT

1.   Vendor Information

FIELD	DETAILS
Company Name	
Business Address	
Satellite/branch Offices (if any)	
Website	
Primary Contact Person	
Position/Designation	
Email Address	
Mobile Number	
Company TIN	
SEC/DTI Registration No.	
Date Established	
Years in Operation	

2.   Type of Business Entity

BUSINESS TYPE	CHECK (✓)
Sole Proprietorship	
Partnership	
Corporation	
Joint Venture	
Other (Please specify): _____	

3.   Accreditation Requirements Checklist

DOCUMENT/REQUIREMENT	SUBMITTED	REMARKS
Company Profile	☐	
SEC/DTI Registration	☐	
BIR Registration & TIN	☐	
Mayor's/Business Permit	☐	
Company Profile	☐	
Audited Financial Statements (Last 2 years)	☐	
List of Key IT Personnel (with CVs)	☐	
List of Current/Past Clients	☐	
Signed NDA or Confidentiality Agreement	☐	
Service Level Agreement (SLA)	☐	

4. Services Offered (Please check applicable)

SERVICE CATEGORY	CHECK (✓)
Software Development	
IT Hardware Supply	
Cloud Services	
Cybersecurity Solutions / Services	
Network & Infrastructure	
IT Consultancy / Training	
Managed IT Services	
Technical Support & Maintenance	
Data Center / Hosting	
Others (Specify): _____	

Rating Scale:

5 – Excellent | 4 – Very Good | 3 – Satisfactory | 2 – Needs Improvement | 1 – Unsatisfactory

6. Final Recommendation

ACCREDITATION STATUS	CHECK (✓)
Approved for Accreditation	
Approved with Conditions	
Not Approved	

Prepared By:

Name: _____

Position: _____

Signature: _____

Date: _____

Reviewed By:

Name: _____

Position: _____

Signature: _____

Date: _____

Approved By:

Name: _____

Position: _____

Signature: _____

Date: _____

Annex 2: IT VENDOR PERFORMANCE ASSESSMENT

CRITERIA	DESCRIPTION	RATING (1-5)	REMARKS
Service Quality	Was the service delivered as expected?		
Timeliness	Was the delivery on time?		
Communication	Was communication clear and responsive?		
Technical Expertise	Did the vendor demonstrate sufficient skill?		
Problem Resolution	Were issues resolved efficiently?		
Documentation	Were reports and documents complete and clear?		
Cost Efficiency	Was the service cost-effective?		
Overall Satisfaction	Overall performance of the vendor		

FINAL EVALUATION SUMMARY:

- **Total Score (out of 40):** _____
- **Average Rating:** _____

FINAL REMARKS:

FINAL DECISION:

☐ **Continue Engagement**
☐ **Put on Probation**
☐ **Discontinue Services**

Annex 3: IT VENDOR PRE-ONBOARDING CHECKLIST

The vendor must demonstrate and provide proof of technical expertise in relevant areas, including but not limited to the following checklist – this will vary depending on the nature of engagement:

CRITERIA	DESCRIPTION	EVIDENCE REQUIRED	COMPLIANT (YES/NO)	REMARKS
1. Domain-Specific Experience	Experience in banking, telecom, retail, government, or other relevant sectors	List of projects, case studies, client references	☐ Yes ☐ No	
2. Industry-Recognized Certifications	Vendor/company holds certifications (ISO, ITIL, PCI DSS, AWS, Microsoft, Cisco, etc.)	Valid certificates, accreditation documents	☐ Yes ☐ No	
3. Specialized Skills	Proven expertise in cybersecurity, cloud, systems integration, or software development (based on project scope)	Staff CVs, skills matrix, technical proposals	☐ Yes ☐ No	
4. Skilled Support & Project Teams	Availability of certified and trained personnel for project execution and support	Org chart, CVs, training certificates	☐ Yes ☐ No	
5. Regulatory & Compliance Expertise	Knowledge of financial/data privacy regulations (e.g., GDPR, BSP, AMLA, local compliance)	Compliance reports, regulatory audit history	☐ Yes ☐ No	
6. Proven Track Record	Successful delivery of similar projects in comparable industries	Case studies, testimonials, project completion certificates	☐ Yes ☐ No	
7. Innovation & Adaptability	Ability to integrate emerging technologies (AI/ML, blockchain, RPA, etc.)	Solution proposals, innovation roadmap	☐ Yes ☐ No	
8. Business Continuity & DR Expertise	Demonstrated capability in resilience planning, disaster recovery, backup testing	DR plans, test reports, certifications	☐ Yes ☐ No	
9. Security & Risk Management	Experience in vulnerability assessment, penetration testing, and risk mitigation	Security reports, certifications, methodologies	☐ Yes ☐ No	
10. Vendor Partnerships	Active partnerships with top technology providers (AWS, Microsoft, Cisco, etc.)	Partnership certificates, reseller/partner status	☐ Yes ☐ No	
11. Training & Knowledge Transfer	Programs to upskill client teams and ensure sustainability post-project	Training plans, sample materials, workshop outlines	☐ Yes ☐ No	
12. Scalability & Performance Optimization	Ability to design solutions that support growth, peak loads, and long-term use	System architecture, scalability case studies	☐ Yes ☐ No	