Vendor Risk Assessment Template

1. **Vendor Details**

Field	Description	Inputs
Vendor Name	Name of the Vendor or Service Provider	
Business Address	Registered Address of the Vendor	
Contact Person & Details	Name, email, and phone number of the vendor's primary contact for security and compliance	
Service provided	Description of the vendors services to SDB bank	
Data Processing Investment	Specify whether the vendor processes personal data, and if so in what capacity (e.g., processor, sub processor)	

2. **Data Sensitivity & Scope of Processing**

Field	Description	Inputs
Categories of Personal Data Processed	Specify the types of personal data involved (e.g., name, NIC number, financial data, health data)	
Special Categories of Data	Does the vendor process sensitive personal data (e.g., health records, biometric data, Children data)?	
Volume of Data	Approximate number of data subjects affected.	

Data Retention Period	How long will the vendor store SDB bank's data?	
Justification for Data Retention	Is the retention period necessary and justified under PDPA requirements?	
Cross-Border Data Transfers	Will any personal data be transferred outside Sri Lanka? If yes, list destination countries and safeguards applied (e.g., Standard Contractual Clauses, adequacy decision)	

3. **Security & Compliance Measures**

Field	**Description**	**Inputs**
Security Certifications & Compliance	List any relevant industry standard certifications (e.g., ISO 27001, SOC 2, PCI-DSS)	
Encryption Practices	Does the vendor encrypt data at rest and in transit?	
Access Controls	Describe role-based access control (RBAC) and multi-factor authentication (MFA) measures implemented	
Data Segregation	Are SDB bank's data stored separately from other clients' data?	
Data Breach Response Plan	Does the vendor have an incident response plan for data breaches? If yes, provide details and response timelines	

Previous Security Incidents	Has the vendor reported any previous data breaches in the last 3 years? If yes, describe them	
PDPA Compliance	Has the vendor confirmed compliance with **Sri Lankan PDPA?**	
Sub-Processors Used	Does the vendor use sub-processors? If yes, are they contractually bound by PDPA-compliant agreements?	

4. **Legal & Contractual Obligations**

Field	**Description**	**Inputs**
Data Processing Agreement (DPA) Signed	Has a DPA been signed between SDB bank and the vendor?	
Vendor's Legal Basis for Processing	What legal basis does the vendor rely on to process personal data (e.g., explicit consent, contract performance, legal obligation)?	
Audit & Monitoring Rights	Does SDB bank have the right to audit the vendor's compliance with PDPA? Does the vendor conduct internal IT audits and how frequently?	
Data Deletion & Return Policy	Upon contract termination, how will the vendor return or delete personal data?	

Liability & Indemnification	What are the vendor's obligations in case of a data breach or non-compliance?	

SDB Bank use only

Risk Rating & Approval

Field	Description	Inputs
Overall Risk Level	Low / Medium / High (based on data sensitivity, security measures, and compliance gaps) - refer to PII metrics for further information	Need to fill by SDB Bank
Risk Mitigation Measures Required	Outline required security or contractual controls before approval	Need to fill by SDB Bank
Approved By	Name and designation of approving officer	Need to fill by SDB Bank
Date of Approval	Date when the vendor assessment was completed and approved	Need to fill by SDB Bank