Sample AI Vendor Due Diligence Questionnaire

FOR INFORMATIONAL USE ONLY *

Purpose: To evaluate the governance, security, regulatory compliance, operational resilience and model risk associated with third-party artificial intelligence (AI) solutions. This **sample** is structured for a bank's vendor management requirements while specifically addressing AI risks. It can be incorporated into an existing Third-Party Risk Management (TPRM) program and scaled based on the criticality of the AI solution under consideration.

Section 1 – Vendor Profile

Item	Response
Vendor Name	
AI Product	
Product Version	
Business Owner	
Bank Department	
Date of Review	
Vendor Contact	
Criticality	Low / Moderate / High / Critical ***(circle one)***
AI Use Case	

AI Use Case

Item	*Select all that apply*
Customer Service Chatbot	
Employee Productivity	
Loan Underwriting Support	
Credit Decisioning	
Fraud Detection	
BSA/AML Monitoring	
Compliance Monitoring	
Marketing	
Call Center Support	
Document Review	
Contract Analysis	
Internal Knowledge Search	
Other	

Section 2 – Regulatory Risk Classification

Does this AI solution:

Item	Yes or No	If Yes – What is Risk Rating? Low/Moderate/High/Critical
Make credit decisions?		
Influence lending decisions?		
Generate adverse action reasons?		
Affect fair lending compliance?		
Interact directly with customers?		
Process Nonpublic Personal Information (NPI)?		
Process Personally Identifiable Information (PII)?		
Process payment information?		
Process confidential supervisory information?		
Support Bank Secrecy Act/AML monitoring?		
Produce regulatory reports?		
Support financial reporting?		
Affect financial statements?		

Section 3 – AI Governance

Does the vendor have:

Item	Yes or No
AI Governance Committee	
Responsible AI Policy	
AI Ethics Policy	
AI Risk Management Framework	
AI Inventory	
AI Change Management Process	
AI Incident Response Plan	
AI Model Validation Process	
AI Performance Monitoring	
Human Oversight Procedures	

Describe the governance structure below:

Section 4 – Model Risk Management

Applicable if predictive or generative AI is used.

Describe the model(s).

Item	Response
Model Name	
Model Type	
Version	
Purpose	
Owner	
Questions	
How is the model trained?	
How frequently is the model retrained?	
What data sources were used?	
How is model drift monitored?	
Can decisions be explained?	
Can outputs be reproduced?	
How are hallucinations detected?	
How are confidence scores calculated?	
How is accuracy measured?	
How is bias monitored?	
Has an independent validation been completed?	
Can the bank perform its own validation?	

Section 5 – Fair Lending and Consumer Protection

Applicable if AI influences lending or customer outcomes.

Describe how the vendor:

Item	Response *(provide supporting documentation when necessary)*
Tests for disparate impact	
Tests for disparate treatment	
Performs bias testing	
Documents explainability	
Supports adverse action notices	
Monitors model fairness	
Reviews protected class impacts	
Maintains audit evidence	
Documents ongoing monitoring	

Section 6 – Data Governance

What data enters the AI system?

Item	*Select all that apply*
Public Information	
Internal Bank Data	
Customer Information	
NPI	
PII	
Transaction Data	
Images	
Audio	
Documents	

Data Controls

Does the vendor:

Item	Yes or No
Use customer prompts to train models?	
Allow training to be disabled?	
Store prompts?	
Store outputs?	
Allow deletion?	
Encrypt data at rest?	
Encrypt data in transit?	
Segregate customer environments?	
Support private cloud deployment?	
Support on-premise deployment?	

Section 7 – Cybersecurity

Confirm the following items have been provided by the vendor:

Item	Yes or No
SOC 2 Type II	
ISO 27001	
Penetration Testing Summary	
Vulnerability Assessment	
Secure Development Lifecycle	
Multi-factor Authentication	
Role-Based Access Control	
Encryption Standards	
Logging	
Monitoring	
Incident Response Procedures	
Cyber Insurance	

Section 8 – Third-Party Risk

Item	Response
Cloud Provider	
Hosting Country	
Sub-processors	
Fourth Parties	
Can the bank audit the vendor?	
Can regulators review documentation?	
Can regulators conduct examinations if required?	
Is there a documented exit strategy?	
How will customer data be returned?	
How will customer data be destroyed?	

Section 9 – Operational Resilience

Item	Response
Recovery Time Objective	
Recovery Point Objective	
Availability SLA	
Disaster Recovery Testing	
Incident Notification Time	
Backup Frequency	
Geographic Redundancy	
Business Continuity Testing	

Section 10 – AI Security Controls

Does the solution provide:

Item	Yes or No
Prompt filtering	
Sensitive data detection	
Data loss prevention	
User authentication	
Session logging	
Audit logs	
Approval workflows	
Human review	
Output monitoring	
Version history	
User permissions	
API security	

Section 11 – Legal & Contractual Review

Verify that contracts address:

Item	Yes or No
Ownership of prompts and outputs	
Confidentiality of customer information	
Compliance with GLBA and applicable privacy laws	
Restrictions on using bank data for model training	
Data retention and deletion requirements	
Right-to-audit provisions	
Regulatory cooperation and examination support	
Service-level agreements (SLAs)	
Breach notification timeframes	
Indemnification	
Intellectual property rights	
Business continuity obligations	
Exit assistance and data portability	

Section 12 – Bank Risk Assessment

Risk Category	Rating *(circle one)*	Mitigating Controls
Strategic Risk	Low / Moderate / High	
Credit Risk	Low / Moderate / High	
Compliance Risk	Low / Moderate / High	
Operational Risk	Low / Moderate / High	
Cybersecurity Risk	Low / Moderate / High	
Model Risk	Low / Moderate / High	
Fair Lending Risk	Low / Moderate / High	
Consumer Protection Risk	Low / Moderate / High	
Reputational Risk	Low / Moderate / High	
Third-Party Risk	Low / Moderate / High	

Section 13 – Required Approval

Function	Approval
Business Owner	
Vendor Management	
Information Security	
Enterprise Risk Management	
Compliance	
Model Risk Management (if applicable)	
Legal	
Internal Audit (if required)	
Executive Sponsor	

Section 14 - Required Supporting Documents

The vendor must provide the following (if applicable):

- AI Governance Framework
- AI Risk Management Policy
- Responsible AI Policy
- Model Cards or Model Documentation
- Independent Model Validation Report
- Bias and Fairness Testing Results
- Explainability Documentation
- Data Flow Diagram

- Data Retention and Deletion Policy
- Secure Software Development Lifecycle (SDLC) Documentation
- SOC 2 Type II Report
- ISO 27001 Certificate
- Penetration Test Executive Summary
- Vulnerability Assessment Summary
- Business Continuity and Disaster Recovery Plans
- Incident Response Plan
- Cyber Liability Insurance Certificate
- List of Sub-processors and Fourth Parties
- AI Change Management Procedure
- Sample Audit Logs
- API Security Documentation

***This sample AI vendor due diligence questionnaire is being provided for INFORMATIONAL USE ONLY to assist members in developing their own questionnaire. The layout and sections used are for demonstration purposes only. Member banks should include appropriate personnel from compliance, legal, etc., as they develop their own questionnaire.**