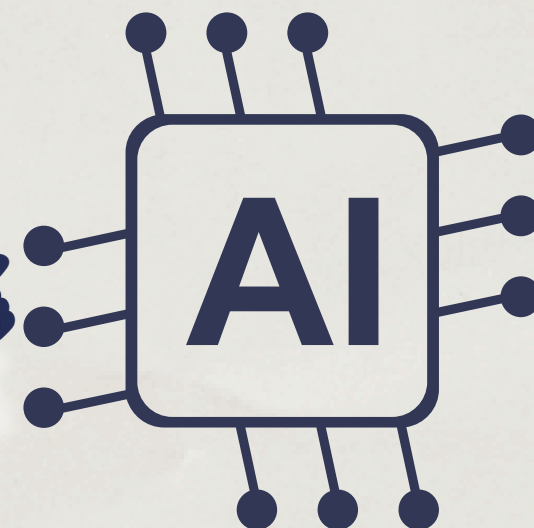




RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE (AI) TOOLS

by: Raj Patel



FINCYBERTECH

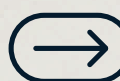
Key Considerations for AI use

A well-structured plan and Policy is essential for ensuring that AI tools are used responsibly and securely at your institution.

Banks should consider:

- Approved AI tools
- Human oversight and training
- Ethical standards and fairness guidelines
- Legal and regulatory requirements
- Transparency and explainability
- AI embedded in 3rd party solutions

Next Page



ACCEPTABLE AI USE CONSIDERATIONS

APPROVED AI TOOLS

Banks should maintain a list of approved AI tools that have been thoroughly vetted for security, compliance, and reliability. This process involves establishing clear criteria for selecting vendors and partners, including a balanced evaluation of their value against potential cyber and compliance risks. Additionally, banks should conduct regular risk assessments and periodic audits of these tools to ensure ongoing compliance and alignment with the bank's high standards for security and regulatory integrity.

ETHICAL & FAIRNESS

AI systems could unintentionally reinforce biases, potentially leading to discriminatory practices, particularly in areas like credit scoring or loan approvals. AI tools must be rigorously tested and monitored to ensure they are free from biases related to race, gender, age, disability, or other protected characteristics. AI systems must never be used to manipulate, deceive, or harm customers, especially in sensitive areas such as personal finance and privacy.

TRANSPARENCY & EXPLAINABILITY

Transparency is essential for building customer trust in AI-driven decisions. Banks should inform customers whenever AI is involved in decision-making processes, such as loan applications or credit evaluations, and emphasize openness in data handling. This includes clearly specifying what data is collected, the purpose of its use, and how it influences decision outcomes.

Contact me at raj@fincybertech.com for help with the safe use of AI at your financial institution or a sample policy.

HUMAN OVERSIGHT & TRAINING

Banks should clearly define situations where human oversight is required, such as adverse lending decisions, to ensure fairness and accountability. Employee responsibilities should also be outlined, emphasizing the importance of monitoring AI systems for potential errors, biases, and anomalies. Additionally, all employees working with AI tools should receive comprehensive training to understand their role in upholding ethical and compliant AI use, fostering a balance between technological efficiency and responsible oversight.

LEGAL & REGULATORY

AI tools must comply with banking-specific laws, including the Gramm-Leach-Bliley Act (GLBA), which mandates the protection of Non-Public Personal Information (NPI). Compliance requirements should also encompass the Bank Secrecy Act (BSA) and the Equal Credit Opportunity Act (ECOA) to ensure comprehensive adherence to regulatory standards.

AI EMBEDDED IN 3RD PARTY APPS

Many banks rely on third-party solutions that incorporate AI technologies. Banks should require vendors to comply with the bank's AI Use Policy and any applicable regulations, including GLBA, BSA & ECOA. To ensure alignment, additional procedures should be integrated into the third-party vendor due diligence process, including compliance assessments and contract language that specifically address AI usage, data protection, and regulatory adherence.

