

البنك المركزي الأردني
CENTRAL BANK OF JORDAN



Artificial Intelligence Framework for Banking Sector in Jordan

Version 1.0 – July 2025

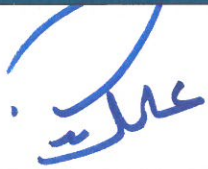
Version	Date	Approved by
July, 2025	V 1.0	

Table of Contents

EXECUTIVE SUMMARY	5
INTRODUCTION	6
SCOPE	6
DEFINITIONS	7
RESPONSIBILITIES	9
TARGET AUDIENCE	9
OBJECTIVES	9
1. GOVERNANCE AND OVERSIGHT	10
1.1 AI GOVERNANCE STRUCTURE	10
1.2 DEFINED RESPONSIBILITIES OF COMMITTEE MEMBERS	10
1.3 RISK-BASED APPROACH	11
2. ETHICS AND TRANSPARENCY	12
2.1 ETHICS AND FAIRNESS	12
2.2 EXPLAINABILITY AND DISCLOSURE	12
2.3 CUSTOMER AUTONOMY AND OPT-OUT RIGHTS	13
2.4 ACCOUNTABILITY	13
2.5 ACCURACY AND BIAS	13
2.6 REGULAR IMPACT ASSESSMENTS	14
3. REGULATORY COMPLIANCE	15
3.1 ALIGNMENT WITH DOMESTIC AND INTERNATIONAL REGULATIONS	15
Domestic Regulations	15
International Compliance and Cross-Border AI Governance	15
3.2 CONFORMANCE TO INTERNATIONAL STANDARDS	15
4. DATA MANAGEMENT	16
4.1 DATA PRIVACY AND PROTECTION	16
Anonymization and Encryption	16
Data Minimization and Retention	16
4.2 DATA QUALITY AND INTEGRITY	16
Data Governance Framework	16
Documentation and Traceability	17
5. SECURE DEVELOPMENT AND DEPLOYMENT	18
5.1 AI SYSTEM SECURITY	18
Secure Lifecycle Approach	18
5.2 MODEL VALIDATION AND TESTING	18
Accuracy, Bias, and Robustness Testing	18

Fail-Safe Mechanisms	19
Calibration.....	19
5.3 CONTINUOUS MONITORING AND AUDITS	19
Ongoing Performance Monitoring.....	19
5.4 HUMAN OVERSIGHT OF AI SYSTEMS.....	20
6. INCIDENT RESPONSE, BUSINESS CONTINUITY, AND DISASTER RECOVERY	21
6.1 INCIDENT MANAGEMENT PLAN	21
AI-Specific Incident Protocols	21
Information Sharing and Regulatory Reporting	21
6.2 BUSINESS CONTINUITY PLANNING	21
Integration with AI Processes	21
Regular Drills and Stress Tests	21
7. THIRD-PARTY RISK MANAGEMENT	22
7.1 VENDOR RISK ASSESSMENTS	22
Due Diligence	22
Diversified Vendor Dependencies and Transparency	22
Contractual Commitments.....	23
8. COOPERATION, AWARENESS, AND TRAINING	24
8.1 STAKEHOLDER ENGAGEMENT	24
International Collaboration.....	24
Capacity Building and Education.....	24
Certification for AI Professionals	24
Awareness Campaigns	24
9. REVIEW AND CONTINUAL IMPROVEMENT	25
Communication and Reporting.....	25
Contact Information.....	25

Executive Summary

The accelerated integration of Artificial Intelligence (AI) across the financial services sector necessitates a structured and adaptive framework to ensure responsible adoption, mitigate associated risks, and unlock long-term value. This document presents a comprehensive AI Framework for the Jordanian banking sector, designed to guide institutions in governing, deploying, and scaling AI capabilities securely and resiliently.

The framework outlines strategic and operational directives across key thematic areas, including: governance, ethics, compliance, data management, security, incident response, and third-party risk. It emphasizes the establishment of a clear AI governance structure, the delineation of responsibilities, and the adoption of a risk-based approach to ensure oversight and accountability at all levels of implementation.

Central to this framework is the integration of ethical principles—such as fairness, explainability, autonomy, and bias mitigation—into AI system design and operations. It also outlines provisions for ensuring transparency, accuracy, and the right for customers to opt out of automated decisions when appropriate.

The framework emphasizes alignment with domestic regulatory expectations while ensuring AI systems conform to recognized standards of privacy, data quality, and operational security. Secure development practices are prescribed through rigorous validation, testing, and continuous monitoring mechanisms to ensure reliability and trustworthiness.

Further, it addresses the need for specialized incident response capabilities, the integration of AI into business continuity planning, and structured third-party risk management protocols to govern vendor relationships and dependencies. The framework also emphasizes stakeholder engagement, capacity building, professional certification, and sustained awareness across all levels of the banking ecosystem.

Finally, the framework sets forth a commitment to ongoing evaluation and refinement, encouraging institutions to embed a culture of continuous improvement, transparency, and innovation as AI maturity evolves within the sector.

This document serves as a foundational blueprint to support the banking sector's strategic transformation through AI, ensuring its deployment aligns with national interests, operational resilience, and public trust.

Introduction

In today's rapidly evolving digital landscape, Jordan's financial sector faces a dual challenge: embracing cutting-edge technological advancements to enhance services while simultaneously addressing complex and emerging risks. Within this complex and fast-evolving environment, Artificial Intelligence (AI) stands out as a transformative force, offering innovative solutions that enhance customer experience, improve risk management, drive business growth, and revolutionize operational processes.

However, integrating AI into financial services is not without its challenges. The potential for biased algorithms, susceptibility to adversarial attacks, and the opacity of AI systems present significant hurdles. Recognizing these challenges, the Central Bank of Jordan (CBJ) is committed to fostering responsible AI adoption, ensuring that innovation goes hand in hand with robust risk management and compliance. A well-structured AI governance framework ensures compliance with national and international regulations while aligning AI initiatives with institutional and sector-wide strategic objectives. Rather than building from scratch, AI governance should leverage existing risk management frameworks, policies, and oversight mechanisms to create a resilient and adaptive regulatory approach that supports both innovation and financial stability.

Building on this foundation, CBJ remains committed to enabling innovation in financial technology while maintaining a secure, stable, and transparent financial ecosystem. By following this framework, banking institutions can confidently leverage AI's transformative potential while aligning with national regulatory objectives and international best practices.

Scope

This framework applies to the use of AI by CBJ-regulated banking institutions. It covers scenarios where an entity develops and implements AI internally, procures AI systems, or outsources processes and functions that directly depend on AI.

Definitions

Accountability	Defined in alignment with the OECD: Accountability refers to the expectation that organizations or individuals will ensure the proper functioning of AI systems, throughout their lifecycle—design, development, operation or deployment, in accordance with their roles and applicable regulatory frameworks, and demonstrating this through their actions and decision-making process (for example, by providing documentation on key decisions throughout the AI system lifecycle or conducting or allowing auditing where justified).
AI System	Defined in alignment with the OECD as: “A machine-based system that, for explicit or implicit objectives, infers from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment”.
Bias	Refers to a systematically better or worse algorithmic performance that leads harm against an individual or sub-population. Sources of such bias can include biases present in training data, design choices, or unintended consequences arising during the deployment of AI systems.
Entity	Refers to CBJ-regulated banking institutions.
Explainability	Defined in alignment with the OECD: Explainability means enabling people affected by the outcome of an AI system to understand how the outcome was reached.
Fairness	Defined in alignment with the OECD: Fairness refers to the commitment to uphold human rights, non-discrimination, and equality throughout the AI system’s lifecycle. It involves ensuring that AI systems are designed and deployed in ways that respect individual dignity, autonomy, and diversity, while preventing bias, exclusion, and unjust outcomes. Fairness also includes implementing safeguards and human oversight to mitigate misuse

	or harm, and to ensure AI operates within ethical and legal boundaries, consistent with democratic values and the rule of law.
Generative AI (GenAI)	Defined in alignment with the OECD definition as: Generative AI (GenAI) is a category of AI that can generate new content such as text, images, videos, and music.
Hallucination	Instances in which generative AI models create seemingly plausible but are factually incorrect.
Impact Assessment	An evaluation process designed to identify, understand, document and mitigate the potential ethical, legal, economic, and societal implications of an AI system in a specific use.
Models	Refers to the specific algorithms used to arrive at AI-driven decisions.
Transparency	Defined in alignment with the OECD: Transparency in AI involves clearly informing individuals when they are interacting with an AI system and providing meaningful, accessible explanations of how the system is developed, how it functions, and how it makes decisions, while respecting technical limitations and proprietary protections.
User	A natural person who may be a consumer or an employee, or a legal person

Responsibilities

The framework is published and owned by the Central Bank of Jordan (CBJ). CBJ is responsible for evaluating and ensuring the effective implementation of this framework across entities, while the entities themselves are accountable for adopting, integrating, and maintaining the framework within their operations. CBJ is also tasked with overseeing its continued alignment with emerging global trends and standards, actively engaging stakeholders to review and revise the framework to reflect the evolving regulatory landscape.

In its role, CBJ is entrusted with safeguarding the confidentiality of sensitive and classified information collected from entities. Any breach of such information will be treated as a security incident and managed in accordance with established incident response protocols.

Target Audience

This framework is intended for all roles within the entity that are involved in the design, development, deployment, and governance of AI systems. These roles include, but are not limited to, the board of directors, senior and executive management, business and information asset owners, risk and compliance officers, AI/ML engineers, data scientists as well as information security and information technology personnel.

Objectives

This framework sets forth the following high-level objectives:

- 1. Promote Responsible and Ethical AI Adoption:** Encourage AI innovation that aligns with Jordanian values, ensuring AI-driven decisions uphold ethical standards.
- 2. Ensure Transparency, Accountability, and Fairness:** Establish mechanisms for explainability and auditability of AI-driven financial products.
- 3. Safeguard Data Privacy, Security, and User Rights:** Protect the confidentiality, security, and integrity of consumer data, in line with national legislation and best international practices.
- 4. Mitigate Financial, Operational, and Reputational Risks:** Establish AI risk management and oversight processes aimed at protecting financial stability and maintaining public trust in AI-enabled services.
- 5. Align with International Standards and Frameworks:** Incorporate applicable global regulatory best practices and foster cross-border cooperation.
- 6. Strengthen AI System Security and Resilience:** Ensure that AI systems are designed, developed, and deployed with robust cybersecurity measures to protect against threats, ensure continuity, and uphold trust in AI-enabled services.

1. Governance and Oversight

This framework emphasizes the establishment of robust AI governance structures.

1.1 AI Governance Structure

- An entity should establish an AI oversight committee or clearly delegate AI governance responsibilities to an existing governance body within the entity.
- **Strategic Alignment:** Each entity should ensure that AI initiatives are aligned with the institution's overall strategic objectives and risk appetite.

1.2 Defined Responsibilities of Committee Members

The AI committee or its equivalent plays a crucial role in governing and guiding the ethical and effective use of AI technologies within the organization. To ensure that critical functions across the AI lifecycle are subject to appropriate board-level governance, the aforementioned committee shall provide high-level direction and oversight in the following key areas:

- **AI Governance and Ethics Oversight:** Oversight of the organization's ethical and strategic approach to AI. This includes approving AI governance frameworks and ensuring that AI policies align with organizational objectives and regulatory requirements, promoting transparency and fairness, overseeing algorithmic design to prevent bias, managing data usage to ensure privacy and compliance, and engaging with stakeholders to uphold legal and ethical standards.
- **Data Management and Governance:** Oversight of enterprise-wide data governance practices to ensure the quality, accuracy, integrity, and compliant use of data across AI systems. This includes supporting AI initiatives through effective data practices and ensuring alignment with data protection regulations.
- **AI Security and Resilience:** Oversight of cybersecurity and resilience measures specific to AI systems. This includes ensuring that security risks are adequately addressed through strategic planning, incident response readiness, business continuity considerations, and embedding appropriate controls throughout the AI lifecycle.
- **AI Technology Integration and Infrastructure:** Oversight of the strategic integration and operational alignment of AI systems within the organization's broader

technology infrastructure. This includes ensuring that AI models are scalable, sustainable, and appropriately maintained, with clear accountability for technical performance and compliance.

- **Regulatory and Legal Compliance:** Oversight of the organization's adherence to legal and regulatory requirements governing AI. This includes cross-border data transfer compliance, oversight of technology partnerships, intellectual property considerations, and alignment with regulations issued by the Central Bank of Jordan (CBJ) and relevant international frameworks.
- **AI Risk Management:** Oversight of AI-related risks within the broader enterprise risk management strategy. This includes guiding the identification, assessment, mitigation, and monitoring of risks related to AI technologies, and ensuring consistency with ethical, regulatory, and strategic standards.

If the organization lacks a dedicated officer or role to oversee these specific responsibilities, it is essential to establish such oversight. In cases where this is not feasible, these responsibilities must be assigned to suitable roles or committees within the organization.

1.3 Risk-Based Approach

To ensure responsible and effective AI governance, each entity must adopt a risk-based approach to manage AI applications. This includes:

- Entity must establish a risk-based framework to classify AI applications based on their potential impact (low, medium, or high risk) and tailor oversight strategies to each classification.
- Entity should incorporate AI risk assessments into the bank's existing risk management framework, ensuring that AI-related risks are evaluated and mitigated alongside traditional risks.
- Entity should define clear lines of accountability to ensure effective governance, compliance, and performance monitoring.
- Entity should adopt AI models incrementally, starting with non-critical systems, rather than deploying them at full-scale immediately to ensure adequate readiness before expanding its use. For critical systems, Human-in-the-Loop (HITL) mechanisms should be integrated to ensure human oversight and intervention where necessary.

2. Ethics and Transparency

To ensure responsible AI deployment, entities must adhere to ethical standards, promote fairness and non-discrimination, and provide clear disclosures about AI usage in decision-making processes.

2.1 Ethics and Fairness

- Entity should design and operate AI systems that respect consumer welfare in accordance with regulations/instructions issued by the Central Bank of Jordan (CBJ).
- Entity should ensure that AI-driven decisions adhere to at least the same ethical standards as human-driven decisions, incorporating principles of fairness, transparency, accountability, and non-discrimination.
- Entity should consider applicable global best practices to support algorithmic fairness and non-discrimination.
- Entity should develop comprehensive AI policies outlining the use, ethical considerations, and compliance requirements for AI technologies, ensuring alignment with the entity's ethical standards, values, and codes of conduct.

2.2 Explainability and Disclosure

- Entity should ensure that AI systems with material impact on customers, such as credit scoring or anti-fraud measures, can produce explainable outputs.
- Entity should communicate AI-driven decision-making processes clearly to relevant stakeholders, where applicable, to foster transparency.
- Entity should provide clear and prominent notifications to customers indicating that they are interacting with AI-driven systems. This disclosure should be made at the point of interaction, ensuring customers are aware that AI models are being used in decision-making processes, including how their data influences the decision and the potential consequences.
- Entity should ensure explainability is tailored to different user groups. General users should receive clear and simplified explanations of AI-driven decisions, technical users should have access to detailed operational insights into AI models, and regulatory authorities should be provided with comprehensive

audit reports on AI decision-making processes to ensure transparency and compliance.

2.3 Customer Autonomy and Opt-out Rights

- Entity should implement clear "opt-out" or alternative service options for customers who prefer not to interact with AI-driven systems - where applicable, providing straightforward procedures for customers to choose traditional or non-AI-based services.
- Entity should ensure that customers have the ability to opt out of AI-driven processes without compromising their access to essential banking services.
- Entity should ensure that customers can access, correct, and request the deletion of their personal data - where applicable, subject to legal and regulatory obligations, particularly for Generative AI systems.

2.4 Accountability

- Entity should ensure that the use of AI systems in decision-making is approved by an appropriate internal authority.
- Entity should be accountable for both internally developed and externally sourced AI-driven decisions.
- Entity should maintain open channels for consumers to question and submit appeals to review AI decisions that affect them.
- Entity should designate an AI System Owner for each AI system, who is accountable for the system's governance, performance, compliance, and ethical alignment throughout its lifecycle.

2.5 Accuracy and Bias

- Entity should regularly review and validate AI data, models, and the AI-driven decisions they produce to detect and mitigate biases, ensuring fairness in outcomes.

2.6 Regular Impact Assessments

- Entity should conduct periodic AI Impact Assessments proportional to the risk level of the application, evaluating privacy risks, potential biases, or any deviation from intended use or fairness objectives, with higher-risk AI requiring more frequent and in-depth reviews to ensure ethical and responsible deployment.

3. Regulatory Compliance

These practices ensure that the design, development, and deployment of AI systems adhere to applicable laws, regulations, and industry standards.

3.1 Alignment with Domestic and International Regulations

Along with this framework, the entity should ensure adherence to mentioned regulations below and their subsequent amendments:

Domestic Regulations

- All applicable regulations, guidelines, frameworks, circulars, and sector-specific security regulations issued by the Central Bank of Jordan (CBJ).
- All national cybersecurity and data privacy laws and guidelines issued by relevant authorities, including Personal Data Protection Law No. (24) of 2023.

International Compliance and Cross-Border AI Governance

Institutions operating internationally or partnering with foreign institutions must assess and incorporate relevant local AI-specific requirements to guarantee cross-border compliance.

Policies should be established to regularly monitor and address changes in the regulatory landscape, both domestically and internationally, ensuring that AI systems remain compliant across all jurisdictions.

3.2 Conformance to International Standards

- Entity is encouraged to adopt applicable international best practices, such as ISO/IEC standards and the Bank for International Settlements (BIS), Financial Services Information Sharing and Analysis Center (FS-ISAC), Organization for Economic Co-operation and Development (OECD), and International Monetary Fund (IMF) guidelines, where relevant, to ensure effective AI risk management, information security, and quality control.

4. Data Management

The framework outlines best practices for data privacy, protection, quality, and integrity. Entities must implement robust data governance policies and ensure the ethical use of data.

4.1 Data Privacy and Protection

Anonymization and Encryption

- Entity should limit training AI models with highly confidential or Personally Identifiable Information (PII) unless necessary and ensure it is appropriately safeguarded.
- Entity should employ anonymization, pseudonymization, or other privacy-preserving techniques to minimize the risk of unauthorized data exposure.
- Entity should also adopt strong encryption for data at rest and in transit, consistent with recognized standards, to ensure data security and confidentiality.
- Entity should implement strict data access controls to ensure that only authorized personnel have access to data used in AI systems.

Data Minimization and Retention

- Entity should collect only the minimum amount of data necessary for AI-driven processes, retaining such data strictly for the duration required to fulfill stated purposes.
- Entity should periodically purge or securely archive data that is no longer essential, thoroughly documenting these processes to ensure compliance and accountability.

4.2 Data Quality and Integrity

Data Governance Framework

- Entity should implement robust data governance policies, overseen by the Chief Data Officer (CDO) or an appropriate senior management role, to ensure the accuracy, completeness, timeliness, availability, and consistency of data.

- Entity should incorporate best practices for continuous data quality; ensuring data is representative, relevant, up-to-date, accurate, and consistent across all systems. Additionally, entities should carefully assess historical data to prevent outdated or biased patterns.

Documentation and Traceability

- Entity should facilitate traceability and accountability by ensuring that all data, models, decisions, user prompts, and authorized overrides are logged and auditable.
- Entity should maintain clear records of data sources, cleaning/preprocessing techniques, and version controls for training and testing sets.
- Entity should store logs in a secure, tamper-evident manner to preserve integrity for regulatory audits or investigations.

5. Secure Development and Deployment

Security measures are emphasized across the AI lifecycle, from design to operation. Entities must integrate robust security protocols, conduct regular testing, and ensure continuous monitoring of AI systems.

5.1 AI System Security

Secure Lifecycle Approach

- Entity should enforce cybersecurity measures outlined in **the Cybersecurity Framework for Jordan's Financial Sector**, safeguarding AI systems from a wide range of emerging threats and vulnerabilities across all operational stages.
- Entity should integrate robust security measures across the AI system's entire lifecycle, including but not limited to Least Privilege, Security by Design, Zero Trust, Secure Coding Practices, Vulnerability Assessment, DLP, Continuous Testing, Deployment Controls, and Advanced Intrusion Detection. This holistic security approach should extend to APIs and their unusual use patterns, underlying infrastructure, data pipelines, and model management, ensuring that the AI system remains resilient against threats from development to decommissioning.
- Entity should store model assets, such as training data and model parameters, in secure environments, implementing logging and change management procedures to ensure integrity and accountability.

5.2 Model Validation and Testing

Accuracy, Bias, and Robustness Testing

- Entity should validate AI models against structured test scenarios and real-world conditions, measuring performance metrics such as accuracy, precision, and recall.
- Entity should assess the robustness of AI systems through comprehensive testing methods, such as out-of-sample testing, benchmarking, sensitivity analysis, stress testing, data diversity testing, edge case evaluation, concept drift analysis, and interoperability testing.

- Entity should integrate adversarial learning techniques to enhance the resilience of AI models against potential attacks or manipulations. These techniques should be incorporated into both the training and testing phases to ensure systems can withstand adversarial inputs.
- Entity should conduct regular penetration testing and vulnerability assessments of AI services and supporting infrastructure, including hallucination and jailbreaking for Generative AI Models.

Fail-Safe Mechanisms

- Entity should design AI systems to include fallback procedures or human review, preventing systemic errors or misuse.
- Entity should develop contingency strategies, including a kill switch, for immediate human intervention in case of system malfunctions, particularly for critical applications to prevent significant errors or misuse.
- Entity should implement Human-on-the-Loop (HOTL) mechanisms to ensure continuous human oversight of AI systems during their operation, especially for critical applications.
- Entity should remediate detected issues swiftly, documenting solutions and accepted risks where necessary.

Calibration

- Entity should update models as market conditions, regulations, and user behaviors evolve.

5.3 Continuous Monitoring and Audits

Ongoing Performance Monitoring

- Entity should continuously monitor AI performance, adjusting the level of monitoring based on the use case and risk level. Automated alerts should be employed where it is feasible to flag anomalies or drift in model accuracy, ensuring timely intervention and risk mitigation.
- Entity should regularly assess, evaluate and document the performance of AI systems.

5.4 Human Oversight of AI Systems

- Entity should incorporate Human-in-the-Loop (HITL) and Human-on-the-Loop (HOTL) mechanisms proportionally to the criticality and risk level of AI systems. Critical systems should include provisions for direct human oversight and intervention when necessary, while higher-risk systems should be subjected to continuous human monitoring throughout AI operations.

6. Incident Response, Business Continuity, and Disaster Recovery

Entities are advised to develop incident management plans, establish clear roles and responsibilities, and ensure business continuity in the face of AI-driven disruptions.

6.1 Incident Management Plan

AI-Specific Incident Protocols

- Entity should develop procedures for AI related incidents or incorporate its existing incident response, as mandated by relevant frameworks and standards.

Information Sharing and Regulatory Reporting

- Entity should establish and maintain a central AI Incident Registry to record incidents, vulnerabilities, and security concerns pertaining to AI implementations.
- Entity should notify FinCERT/CBJ promptly of any AI-related incidents in accordance with any instructions issued by CBJ in this regard.
- Entity should share threat intelligence and best practices across the financial sector community to align with the evolving AI risks.

6.2 Business Continuity Planning

Integration with AI Processes

- Entity should update business continuity and disaster recovery plans to account for AI applications deemed critical for day-to-day banking operations.

Regular Drills and Stress Tests

- Entity should conduct scenario-based drills, including worst-case scenarios of AI failures or targeted cyberattacks.
- Entity should evaluate its readiness to minimize service disruption and protect critical infrastructure.

7. Third-Party Risk Management

These practices involve evaluating and overseeing external vendors and service providers that contribute to an organization's AI systems.

7.1 Vendor Risk Assessments

Due Diligence

- Entity should perform rigorous evaluations of external AI solutions, ensuring that vendors comply with CBJ and other relevant domestic regulations, based on the criticality of the AI model.
- Entity should verify credentials, data security safeguards, and documented track records of managing AI models responsibly.
- Entity should ensure that third party vendors entrusted with outsourced responsibilities possess the necessary skills and experience.
- Entity should assess the transparency and explainability of AI models, ensuring that the vendor can provide understandable explanations of AI decision-making processes where feasible.
- Entity should evaluate the vendor's methods for identifying and mitigating biases in AI models to prevent discrimination.
- Entity should verify that the vendor employs robust testing and validation procedures to ensure AI model accuracy and reliability.
- Entity should ensure that the vendor maintain a clear process for AI model updates and maintenance, including handling deprecated components or technologies.
- Entity should confirm the vendor's commitment to ethical AI practices, such as fairness, accountability, and transparency in AI operations.

Diversified Vendor Dependencies and Transparency

- Entity should be vigilant about concentrations in vendor dependencies and ensure a diverse selection of AI solution providers when possible. By incorporating different approaches, technologies, and vendors into their ecosystem, the entity can mitigate the risks associated with herding behavior,

avoid over-reliance on a single vendor or small group of vendors, and ensure resiliency.

- Entity should require third-party vendors, when applicable, to provide an AI Bill of Materials (AIBOM) for all AI systems or solutions supplied.

Contractual Commitments

- Entity should incorporate explicit clauses on responsibilities and liability issues, data privacy, intellectual property rights, bias mitigation, explainability, and compliance with relevant standards.
- Entity should ensure that contracts with vendors include audit rights, allowing the entity to conduct audits or receive audit reports from qualified auditors.
- Entity should ensure that contracts with vendors include provisions for cooperation during investigations and/or incident response. This should guarantee timely access to necessary information, and technical support.
- Entity should create comprehensive exit strategies, to ensure the smooth transfer of data and knowledge in the event of contract termination.
- Entity should ensure minimal disruption to AI-enabled services during vendor transitions.

8. Cooperation, Awareness, and Training

Stakeholder engagement and continuous education are essential for staying informed and prepared. The framework encourages collaboration with local and global AI communities and emphasizes the importance of professional AI certification and public awareness campaigns.

8.1 Stakeholder Engagement

International Collaboration

- Entity should actively engage with local and global AI communities, international regulatory bodies, and working groups to stay informed about industry trends, share knowledge and intelligence, and collaborate on best practices.

Capacity Building and Education

- Entity should provide ongoing education for all personnel involved in the AI lifecycle, including data scientists, auditors, developers, security staff, compliance officers, and executives, on topics such as AI risk management, ethics, bias mitigation, explainability, emerging AI threats, and cybersecurity.

Certification for AI Professionals

- Entity should encourage or require staff certifications in AI governance, risk assessment, and security.

Awareness Campaigns

- Entity should conduct public awareness initiatives to inform customers about AI-driven banking services, data privacy, and consumer rights.
- Entity should provide customers with guidance on the appropriate use of the system or model.

9. Review and Continual Improvement

Improvement is a continuous process. A technology evolves rapidly, the composition of the financial sector also changes over time with new types of entities, products, and/or services emerging, and increased reliance third-party service providers. CBJ shall review the AI framework and related documents and tools biennially.

Entities may also request updates to the framework by submitting a formal application approved by their AI management and the AI committee.

Communication and Reporting

Entities should designate representatives to communicate and coordinate with the CBJ regarding the implementation of this framework. These representatives must include, at a minimum, the Head of Chief AI Officer (CAIO), or any relevant position.

Contact Information

All communications from the designated representatives of member entities should be addressed to: fincert@cbj.gov.jo.