AI Governance Guide for Lebanese Financial Institutions

A Framework for Responsible AI Adoption and Management in the Lebanese Financial Sector

Version: 2.0
Date: November 12, 2025
Author: Abed Al Rahman Naboulsi, Information Security Officer
Published by: Capital Outsourcing SAL

Important Disclaimer

This guide provides general guidance based on the interpretation of existing regulations and international best practices as of November 2025. It is not a substitute for professional legal, financial, or specific compliance advice. Regulatory requirements are subject to change and interpretation. Always consult with Banque du Liban (BDL) directly and seek specific legal and compliance advice from qualified professionals for implementation decisions. Each institution remains solely responsible for ensuring that its adoption and implementation of AI systems comply with applicable laws, regulatory requirements, ethical standards, and its own internal or faith-based principles. The author and affiliated entities disclaim liability for any loss or damage arising from use of or reliance on this guide. This guide is provided under CC BY 4.0; institutions should adapt content to their specific context.

Table of Contents

1. Executive Summary

1.1 Context and Challenge

Lebanese financial institutions are at a critical juncture, navigating the dual pressures of digital transformation and a complex, evolving regulatory environment. The advent of Artificial Intelligence (AI) offers unprecedented opportunities for innovation, efficiency, and enhanced customer experience [1]. At the time of writing, Banque du Liban (BDL) has not yet published AI-specific regulations; this means institutions must carefully interpret existing rules when applying them to AI systems. Financial institutions must innovate responsibly by interpreting and applying existing legal and regulatory frameworks to their AI systems.

This guide offers a practical framework to support institutions in adopting AI responsibly while maintaining governance, risk management, and compliance with applicable requirements. It builds upon existing regulatory interpretations and best practices, including those detailed in the Lebanese FinTech BDL Compliance Guide by Abed Al Rahman Naboulsi [2], which provides a foundational understanding of BDL compliance for technology-driven financial services.

The regulatory landscape in Lebanon contains particular features institutions should consider when implementing AI in financial services. Unlike jurisdictions such as the European Union, which has developed comprehensive AI-specific legislation through the EU AI Act [3], or the United States, which has established frameworks through the NIST AI Risk Management Framework [4], Lebanon relies on the interpretation and extension of existing banking and technology regulations to govern AI systems.

It is crucial to acknowledge that Lebanese financial institutions operate within a uniquely challenging economic environment. The recommendations in this guide, particularly the implementation roadmap, should be viewed as an aspirational framework. Institutions must adapt these guidelines pragmatically, prioritizing actions based on a risk assessment that considers their specific resource constraints, infrastructure stability, and talent availability

1.2 Key Regulatory Constraints

The foundation of AI governance in Lebanon is built upon existing laws and BDL circulars, which institutions must carefully interpret to address AI-specific issues. The key regulatory constraints include:

Banking Secrecy Law (1956): Lebanon's Banking Secrecy Law of 1956, inspired by the Swiss model, established strict confidentiality requirements for customer data [5] to attract investment and protect financial privacy. While the law included some exceptions (e.g., client consent, bankruptcy, illicit enrichment lawsuits), it generally imposed stringent secrecy obligations. This foundational principle of data secrecy has been a cornerstone of the Lebanese banking sector and continues to influence data handling, with significant

implications for AI systems, particularly regarding data sharing for model training, cross-border data transfers, and the use of cloud-based AI services.

Amendment to Banking Secrecy Law (Law No. 306 of 2022 and Subsequent Amendments): Driven by the country's financial crisis and as a prerequisite for an IMF program, Lebanon significantly amended the 1956 Banking Secrecy Law through Law No. 306, passed in October 2022. This legislation, along with further amendments approved in April 2025 following Decree No. 103 on April 2, 2025, expands exceptions to banking secrecy. It empowers a range of state and independent bodies, including the Central Bank (BDL), the Banking Control Commission (BCC), the Special Investigation Commission (SIC), the National Deposit Insurance Institution (NDII), and authorized independent auditors to access client names, account balances, and transaction histories for forensic audits, bank restructuring, and investigations of financial crimes. The law applies retroactively, generally to 2015. The April 2025 amendments granted the BCC greater authority to access bank account data, including account holders' names. The IMF has cited 'key deficiencies' in the initial 2022 law, seeking broader access to government agencies and expressing concern that harsh penalties might deter whistleblowers.

BDL Basic Circular 69/2000: This circular governs **electronic banking operations** and requires prior notification or approval from Banque du Liban for offering such services [6]. While BDL Basic Circular 69/2000 does not explicitly mention AI, its principles governing electronic banking services are highly relevant. Institutions should therefore interpret its requirements to apply to customer-facing AI systems like chatbots, digital onboarding tools, and robo-advisors.

BDL Basic Circular 144/2017: This circular establishes the framework for **cybersecurity and cybercrime prevention** [7]. It requires financial institutions to implement governance structures, technical controls, incident-response procedures, and cyber-insurance coverage. These requirements extend to AI environments, ensuring that data protection, access control, and resilience mechanisms are integrated into AI system design and operation.

BDL Basic Circulars 123/2009 & 141/2017: Circular 123/2009 establishes core governance, risk-management and internal audit expectations for banks; **Circular 141/2017** requires a Board-approved Recovery Plan that identifies critical business functions, responsibilities, activation triggers and recovery strategies (including stress-testing) [7]. Interpreting these instruments together for AI, institutions should treat AI systems that support critical functions as both model-risk and operational-resilience assets: include them in governance and model-validation programs (documentation, performance and bias testing, auditability) and in recovery/continuity arrangements (dependency mapping, backups, fallback/manual processes, model restoration strategies and stress tests). (This is an interpretative application of existing circulars to AI systems and should be confirmed with BDL where appropriate.)

BDL Basic Circular 128/2013: This circular establishes the **compliance and outsourcing governance framework** [9]. It requires banks to create independent compliance functions, manage outsourcing risks, and ensure accountability for third-party service providers. These

principles directly apply to AI-related outsourcing, particularly when using external data analytics, AI models, or cloud platforms.

BDL Basic Circular 146/2018: This circular introduces **data protection and customer information privacy** requirements [10]. It strengthens confidentiality obligations and mandates financial institutions to adopt safeguards aligned with international privacy standards, such as purpose limitation, consent management, and secure data transfers. Its provisions are critical for AI systems processing customer data or leveraging cloud-based infrastructure.

Data Sovereignty: Derived from the Banking Secrecy Law and general BDL oversight, the principle of data sovereignty effectively establishes requirements that sensitive financial data remains within Lebanese jurisdiction [11]. This has significant implications for the use of international public cloud services for AI, requiring careful consideration of data residency, processing locations, and cross-border data transfer mechanisms.

Law 81/2018: This law establishes a framework for electronic transactions and personal data protection [12], introducing data subject rights and security requirements that are highly relevant to AI. The law's provisions for consent, data minimization, and individual rights create additional compliance obligations for AI systems that process personal data.

1.3 Strategic Approach

To navigate this complex landscape, this guide proposes a pragmatic, three-pillar strategic approach:

Regulatory Interpretation: This involves a careful and documented interpretation of existing BDL requirements and their application to AI systems. This approach ensures that the institution's AI initiatives are grounded in a solid understanding of the current regulatory landscape. The interpretation process requires collaboration between legal, compliance, and technical teams to ensure that AI implementations meet both the letter and spirit of existing regulations.

International Alignment: While specific local regulations have not yet been published, it is prudent to selectively adopt principles from established international standards and frameworks. This guide draws on best practices from ISO 42001 [13], the EU AI Act [3], and the NIST AI Risk Management Framework [4], among others. This alignment not only enhances the robustness of the governance framework but also prepares the institution for future regulatory developments that may incorporate international standards.

Practical Implementation: The guide emphasizes a focus on achievable, risk-based controls. It provides practical tools, checklists, and templates to facilitate the implementation of the proposed governance framework. The implementation approach recognizes the resource constraints and operational realities faced by Lebanese financial institutions while maintaining high standards of governance and risk management.

1.4 Key Principles

The following key principles form the bedrock of the recommended AI governance framework:

Data Processing Prioritization: Prioritizing the use of Lebanese infrastructure for data processing, especially for sensitive data, is a key principle derived from data sovereignty requirements [14]. This principle guides decisions about cloud service selection, data center locations, and cross-border data transfer mechanisms. Institutions should establish clear criteria for determining when local processing is required and develop technical architectures that support data sovereignty compliance.

BDL Notification or Approval: All customer-facing AI systems or those that have a significant impact on regulated services require notification to or approval from BDL, in line with BDL Basic Circular 69/2000 [6]. This principle ensures regulatory transparency and allows BDL to maintain oversight of technological developments in the banking sector. Institutions should establish clear processes for identifying systems that require prior approval and develop comprehensive documentation packages for regulatory submissions.

Institutional Accountability: The financial institution remains fully accountable for its AI systems, regardless of whether they are developed in-house or procured from third-party vendors, as per BDL Basic Circular 128/2013 [9]. This principle emphasizes that outsourcing AI development or deployment does not transfer regulatory responsibility. Institutions must maintain appropriate oversight, control, and risk management capabilities for all AI systems, regardless of their source.

Human Oversight: Meaningful human oversight is essential for high-risk AI decisions and critical automated processes [15]. This principle, aligned with global best practices, ensures that human judgment remains a key component of the decision-making process. Institutions should implement appropriate human-in-the-loop mechanisms, establish clear escalation procedures, and maintain the ability to override or intervene in AI-driven decisions when necessary.

Ethical AI Principles: A commitment to developing and deploying AI systems that are fair, transparent, accountable, and respect human rights and societal values is a fundamental tenet of responsible AI [16]. This principle guides the design, development, and deployment of AI systems to ensure they align with societal expectations and ethical standards. Institutions should establish clear ethical guidelines, implement bias detection and mitigation measures, and regularly assess the societal impact of their AI systems.

2. Lebanese Regulatory Landscape for AI

Lebanon's regulatory environment for financial institutions, while not yet featuring explicit AI-specific legislation, provides a foundational framework through existing laws and Banque du Liban (BDL) circulars. These regulations, originally designed for traditional banking operations and IT systems, must be carefully interpreted and applied to the unique characteristics and risks of Artificial Intelligence. This section details the direct regulatory

requirements, the broader legal framework, and identifies current regulatory areas where guidance is not explicit and their practical interpretations.

2.1 Direct Regulatory Requirements

2.1.1 BDL Basic Circular 69/2000

Applicability to AI: BDL Basic Circular 69/2000, issued on March 27, 2000, governs electronic banking and financial operations [6]. Its broad scope means that any AI system that directly interfaces with customers, facilitates electronic transactions, or significantly impacts customer services falls under its purview. This includes chatbots, robo-advisors, automated loan application processing systems, fraud detection systems, and algorithmic trading platforms. The circular aims to ensure the security, integrity, and reliability of electronic services offered by financial institutions.

The interpretation of this circular in the context of AI systems requires careful consideration of what constitutes an "electronic banking service." Modern AI applications often blur the lines between traditional service categories, requiring institutions to adopt a conservative approach in determining applicability. For instance, an AI-powered customer service chatbot that can access account information and perform basic transactions clearly falls under the circular's scope, while a purely informational AI assistant may require case-by-case evaluation.

Requirements:

Where notification or approval is required by the circular, institutions should engage proactively with BDL and provide clear documentation demonstrating controls and safeguards [6]. This extends to customer-facing AI implementations or those that significantly impact regulated services. Institutions must demonstrate that adequate security measures and controls are in place before deployment. The approval process typically involves a comprehensive review of the system's technical architecture, security controls, risk assessment, and operational procedures.

The approval process for AI systems presents unique challenges due to the complexity and evolving nature of AI technologies. Traditional IT systems often have predictable behaviors and well-defined operational parameters, while AI systems may exhibit emergent behaviors and require continuous learning and adaptation. This necessitates a more dynamic approach to regulatory approval, potentially involving ongoing monitoring and periodic re-evaluation of approved systems.

Technology Infrastructure Assessment: The circular establishes requirements for the submission of a comprehensive Technology Infrastructure Assessment to BDL [6]. For AI systems, this assessment must detail:

- **System Architecture and Data Flows:** A clear outline of how the AI system is designed, its components, and how data flow through it, including interactions with existing banking systems. This includes documentation of the AI model architecture,

training data sources, inference pipelines, and integration points with core banking systems.

- **Security Measures:** Detailed descriptions of security controls implemented to protect the AI system, its data (training, input, output), and its underlying infrastructure. This encompasses traditional cybersecurity measures as well as AI-specific security considerations such as model protection, adversarial attack prevention, and data poisoning mitigation.
- **Risk Assessment:** A thorough analysis of potential risks associated with the AI system, including operational, security, and compliance risks, along with proposed mitigation strategies. AI-specific risks include model bias, algorithmic discrimination, explainability challenges, and potential for unintended consequences.
- **Business Continuity Plans (BCP):** How the AI system is integrated into the institution's overall BCP, ensuring resilience and recovery capabilities in case of disruption [6]. This includes fallback procedures for AI system failures, manual override capabilities, and data backup and recovery procedures for AI models and training data.

Documentation Needed: To obtain BDL approval, financial institutions are typically required to provide extensive documentation [6]. For AI systems, this documentation package should include:

- Technical specifications detailing the AI model architecture, algorithms used, and performance characteristics.
- Detailed risk assessment reports covering both traditional IT risks and AI-specific risks.
- Results from security audits, including penetration testing and vulnerability assessments.
- User acceptance testing (UAT) results, demonstrating system functionality and reliability.
- Model validation reports showing accuracy, fairness, and robustness testing results.
- Data governance documentation outlining data sources, quality controls, and privacy protections
- Operational procedures for model monitoring, maintenance, and updates

2.1.2 BDL Basic Circular 144/2017

Standard Requirements Applicable to AI: BDL Basic Circular 144/2017, issued on November 15, 2017, establishes requirements for comprehensive cybersecurity measures for financial institutions [7]. This circular is directly applicable to AI systems as it establishes a baseline for the protection of all information systems and data. The circular's requirements take on additional complexity when applied to AI systems due to their unique characteristics and attack vectors.

Key Requirements:

Encryption: Mandatory encryption of data at rest and in transit, utilizing strong cryptographic algorithms (e.g., AES-256) and secure communication protocols (e.g., TLS 1.2+) [7]. This applies to AI training data, model parameters, and inference data. For AI systems, encryption considerations extend beyond traditional data protection to include:

- Protection of proprietary AI models and algorithms.
- Secure transmission of model updates and parameters.
- Encryption of large-scale training datasets.
- Protection of real-time inference data streams.

Access Control and Authentication: Implementation of robust access control mechanisms, including multi-factor authentication (MFA) for privileged access [7]. For AI systems, this includes controlling access to:

- AI model development environments.
- Training data repositories.
- Model deployment and inference systems.
- AI system monitoring and logging interfaces.
- Model update and versioning systems.

Vulnerability Management and Penetration Testing: Regular vulnerability assessments and penetration testing of AI systems and their supporting infrastructure [7]. AI-specific vulnerability assessments should include:

- Testing for adversarial attacks and input manipulation.
- Assessment of model robustness and stability.
- Evaluation of data pipeline security.
- Testing of AI-specific APIs and interfaces.

Incident Response Procedures: Establishment of clear and tested incident response procedures for cybersecurity incidents, including prompt reporting to BDL [7]. AI-specific incident response procedures should address:

- Model performance degradation or failure.
- Data breaches involving training data.
- Adversarial attacks on AI systems.
- Unauthorized model access or theft.
- Bias or discrimination incidents.

Continuous Security Monitoring and Logging: Implementation of continuous monitoring and comprehensive logging of activities within AI systems [7]. This includes:

- Model performance monitoring and drift detection.
- Access logging for AI systems and data.
- Anomaly detection in AI system behavior.
- Audit trails for model updates and changes.

AI-Specific Considerations (Interpretation): While Circular 144 does not explicitly mention AI, its principles extend to AI systems, requiring specific considerations such as:

Protection of Training Data and Model Integrity: Ensuring the confidentiality, integrity, and availability of large datasets used for AI model training, and protecting models from unauthorized modification or tampering. This includes implementing data lineage tracking, version control for models and datasets, and integrity verification mechanisms.

Robust API Security: Implementing stringent security measures for Application Programming Interfaces (APIs) used for model serving and integration with other systems. AI APIs often handle sensitive data and provide access to valuable intellectual property, requiring enhanced security measures including rate limiting, input validation, and output filtering.

Protection Against AI-Specific Attacks: Addressing emerging threats like adversarial attacks (manipulating input data to cause incorrect outputs) and data poisoning (injecting malicious data into training sets to compromise model integrity) [17]. These attacks represent novel threat vectors that traditional cybersecurity measures may not adequately address.

2.1.3 BDL Basic Circular 123/2009

Banks must maintain robust risk-management, audit, governance and oversight frameworks for their operations. Within this framework, AI systems that support core financial services must be treated as a component of the institution's risk environment: subject to documentation, monitoring, change-control, auditability and transparency.

2.1.4 BDL Basic Circulars 123/2009 & 141/2017

Banks are required to prepare a Board-approved Recovery Plan, tailored to their size/complexity, that identifies critical business functions, assigns responsibilities, defines activation triggers, and specifies recovery strategies (including stress-testing). AI systems underpinning critical functions (such as credit decisions, fraud detection, customer transaction monitoring, algorithmic trading support, etc.) should therefore be included in the institution's recovery framework: their dependencies, data inputs, model logic, vendor or internal infrastructure, fallback modes (e.g., manual processing) must be identified and planned for.

Practically, this means an institution should:

1. *Identify which AI systems support functions that the board would consider "critical" for recovery.*
2. *Map dependencies of those AI systems: data pipelines, IT infrastructure (servers, networks, cloud), external vendors, algorithms/ML models, regulatory interfaces, customer channels.*
3. *Define recovery strategies for each system/component: e.g., backup model versions, fallback to non-AI/manual processes, alternate sites, remediation of model bias or drift, cyber-attack recovery.*

4. *Assign roles and responsibilities: model risk manager, AI operations lead, data governance lead, IT disaster recovery lead, business continuity lead, communications to stakeholders.*
5. *Develop triggers/indicators for activation: e.g., model performance degradation beyond threshold, data pipeline failure > X hours, vendor service interruption, major regulatory breach.*
6. *Conduct stress-tests and scenario analyses: scenarios such as AI system failure, mass customer complaint due to AI decision error, adversarial attack leading to incorrect outcomes, cascading IT outage, third-party vendor collapse.*
7. *Ensure board oversight and periodic review: board approves the recovery plan, reviews test results, ensures resources, ensures alignment with risk management and recovery plan.*

AI-Specific Business Continuity Considerations:

Model Availability and Redundancy: AI systems that are critical to business operations must have appropriate backup and redundancy mechanisms. This includes maintaining multiple instances of AI models, implementing failover procedures, and ensuring that model serving infrastructure can handle increased loads during primary system failures.

Data Backup and Recovery: AI systems often depend on large volumes of training data and historical data for proper functioning. Business continuity plans must include procedures for backing up and recovering this data, including considerations for data versioning, incremental backups, and cross-site replication.

Fallback Procedures: When AI systems fail or become unavailable, institutions must have manual or alternative automated procedures to maintain critical business functions. This requires careful documentation of AI system decision-making processes and training staff to handle manual overrides.

Model Retraining and Recovery: In cases where AI models become corrupted or compromised, institutions must have procedures for rapidly retraining or restoring models from clean data sources. This includes maintaining clean training datasets, documented model training procedures, and the computational resources necessary for rapid model reconstruction.

2.1.5 BDL Basic Circular 128/2013

Third-Party AI Services: BDL Basic Circular 128/2013 governs outsourcing arrangements and emphasizes that banks retain full accountability for outsourced functions [9]. This principle is particularly relevant for AI systems, where institutions may rely on third-party providers for various components including cloud infrastructure, pre-trained models, AI development platforms, and specialized AI services.

Key Requirements for AI Outsourcing:

Due Diligence and Vendor Assessment: Institutions must conduct thorough due diligence on AI service providers, including assessment of their technical capabilities, security

measures, compliance frameworks, and financial stability. For AI vendors, this assessment should include evaluation of model development practices, data handling procedures, and intellectual property protections.

Contractual Safeguards: Outsourcing agreements for AI services must include appropriate contractual safeguards, including service level agreements, data protection clauses, audit rights, and termination procedures. AI-specific contractual considerations include model performance guarantees, bias and fairness requirements, and intellectual property ownership.

Ongoing Monitoring and Control: Institutions must maintain ongoing oversight of outsourced AI services, including regular performance monitoring, compliance assessments, and risk evaluations. This includes monitoring model performance, reviewing vendor security practices, and ensuring continued compliance with regulatory requirements.

Exit Strategies: Institutions must have clear exit strategies for AI outsourcing arrangements, including procedures for data retrieval, model migration, and service transition. This is particularly important for AI services where vendor lock-in can create significant operational and strategic risks.

2.2 Broader Legal Framework

2.2.1 Banking Secrecy Law (1956) and Amendments

The Banking Secrecy Law of 1956 remains a cornerstone of Lebanese banking regulation and has significant implications for AI systems that process customer data [5]. However, a series of recent reforms, including Law No. 306/2022 and subsequent amendments approved in April 2025 following Decree No. 103 on April 2, 2025, have significantly reshaped its application. The law's strict confidentiality requirements create both constraints and obligations for AI implementations. While the obligation of professional secrecy for bank managers and employees remains, the amendments have created significant exceptions. Law No. 306, passed in October 2022, along with the April 2025 amendments, empowers a range of state and independent bodies to access banking information. This includes the BDL, the Banking Control Commission (BCC), and the Special Investigation Commission (SIC) for AML/CFT, as well as judicial authorities, granting them the power to lift banking secrecy for investigative and audit purposes. This also includes granting appointed audit firms access to all necessary banking data to evaluate bank balance sheets and investigate potential violations. The law applies retroactively, generally to 2015 [18].

Implications for AI Data Governance: The Banking Secrecy Law requires institutions to implement robust data governance frameworks for AI systems, including:

- **Data Access for Regulators:** Institutions must have the technical capability to securely provide regulators with detailed, granular data from their AI systems, including training datasets, transaction logs, and decision outputs, when requested.
- **Data Sovereignty:** The amendments may create a more defined legal framework. While data sovereignty principles, derived from the Banking Secrecy Law and

general BDL oversight, remain important, the ability to grant regulators access to data stored in secure, audited environments (even if located abroad) may become more feasible, provided the provider can guarantee compliance with Lebanese law.

- **Model Auditability:** AI models, especially those used for credit scoring, risk management, and AML, must be designed for full auditability. This includes logging all inputs, outputs, and the rationale for decisions to comply with potential regulatory investigations.

2.2.2 Law 81/2018 - Electronic Transactions and Data Protection

Law 81/2018 establishes a framework for electronic transactions and personal data protection in Lebanon [12]. This law introduces important concepts and requirements that directly impact AI system design and operation.

Data Subject Rights: The law establishes various rights for data subjects, including rights to access, rectification, and erasure of personal data. For AI systems, this creates obligations to:

- Implement mechanisms for data subject access requests.
- Provide explanations of automated decision-making processes.
- Enable data correction and deletion in AI training datasets.
- Maintain audit trails for data processing activities.

Consent and Lawful Basis: The law requires appropriate legal basis for data processing, including explicit consent for certain types of processing. AI systems must be designed to meet these requirements, including:

- Obtaining appropriate consent for AI training data use.
- Implementing Purpose Limitation for AI data processing.
- Providing clear information about AI system data use.
- Enabling withdrawal of consent where applicable.

Data Security Requirements: The law establishes requirements appropriate technical and organizational measures to protect personal data. For AI systems, this includes:

- Implementing privacy-by-design principles in AI development.
- Conducting privacy impact assessments for AI systems.
- Implementing data protection measures throughout the AI lifecycle.
- Ensuring secure data handling in AI training and inference.

2.3 Regulatory Gaps and Interpretations

2.3.1 AI-Specific Regulations (not yet published - existing regulations require interpretation for AI applications)

The most significant challenge facing Lebanese financial institutions is at the time of writing, Banque du Liban (BDL) has not yet published AI-specific regulations; institutions must

therefore carefully interpret existing rules when applying them to AI systems. This situation requires institutions to exercise care when interpreting regulatory expectations and assessing compliance obligations for AI systems. Institutions must navigate this uncertainty by adopting conservative interpretations of existing regulations and implementing robust governance frameworks.

Interpretive Challenges: The application of traditional banking regulations to AI systems often requires significant interpretation and judgment. Key areas of interpretive challenge include:

- Determining when AI systems require regulatory approval or notification.
- Applying traditional risk management frameworks to AI-specific risks.
- Interpreting data protection requirements in the context of AI training and inference.
- Balancing innovation objectives with regulatory compliance obligations.

Prudent and Consultative Approach: Until further regulatory guidance is issued, institutions are advised to take a prudent, well-documented approach to AI governance and to engage proactively with the regulator where appropriate. This includes:

- Seeking regulatory guidance for novel AI applications.
- Implementing comprehensive governance frameworks that exceed minimum requirements.
- Maintaining detailed documentation of AI system design and operation.
- Establishing clear escalation procedures for regulatory questions.

2.3.2 International Standards Adoption

International frameworks such as the EU AI Act and NIST AI RMF provide useful reference points; Lebanese institutions can draw on these standards while adapting them to local regulatory context. This approach provides several benefits:

- Alignment with global best practices and emerging regulatory trends.
- Preparation for future Lebanese AI regulations that may incorporate international standards.
- Enhanced risk management and governance capabilities.
- Improved stakeholder confidence and trust.

Relevant International Standards:

ISO/IEC 42001:2023 - AI Management Systems: This international standard provides a framework for establishing, implementing, maintaining, and continually improving AI management systems [13]. The standard covers AI governance, risk management, and quality assurance throughout the AI lifecycle.

NIST AI Risk Management Framework: The U.S. National Institute of Standards and Technology has developed a comprehensive framework for managing AI risks [4]. The

framework provides guidance on AI risk identification, assessment, and mitigation across various domains and applications.

EU AI Act: While not directly applicable to Lebanese institutions, the EU AI Act provides valuable guidance on AI risk classification, governance requirements, and compliance obligations [3]. The Act's risk-based approach and technical requirements can inform Lebanese AI governance frameworks.

IEEE Standards for AI: The Institute of Electrical and Electronics Engineers has developed various standards related to AI ethics, transparency, and technical implementation [19]. These standards provide technical guidance for AI system design and operation.

ISO/IEC 27001:2022: The technical and security controls detailed in this guide are not designed to exist in a vacuum. They should be implemented as part of a comprehensive Information Security Management System (ISMS), for which **ISO/IEC 27001:2022** is the international standard. An effective ISMS provides the governance, risk management, and control framework necessary to protect all information assets, including the data and models central to AI systems.

2.3.3 Practical Interpretation Guidelines

To address regulatory areas requiring interpretation and provide practical guidance for AI implementation, institutions should develop clear interpretation guidelines that address common scenarios and use cases.

AI System Classification: Institutions should develop clear criteria for classifying AI systems based on their risk profile, regulatory impact, and business criticality. This classification should inform governance requirements, approval processes, and ongoing monitoring obligations.

Regulatory Notification Thresholds: Clear guidelines should be established for determining when AI systems require regulatory notification or approval. These guidelines should consider factors such as customer impact, data sensitivity, decision-making authority, and integration with critical business processes.

Risk Assessment Frameworks: Institutions should develop comprehensive risk assessment frameworks that address both traditional IT risks and AI-specific risks. These frameworks should provide clear methodologies for risk identification, assessment, and mitigation planning.

Documentation Standards: Clear documentation standards should be established for AI systems, including requirements for technical specifications, risk assessments, validation reports, and operational procedures. These standards should ensure that adequate information is available for regulatory review and ongoing governance.

3. Core Governance Framework

The core governance framework for AI in Lebanese financial institutions is built upon the internationally recognized Three Lines of Defense model, adapted specifically for the unique challenges and risks associated with artificial intelligence systems. This framework ensures comprehensive oversight, accountability, and risk management throughout the AI lifecycle while maintaining compliance with Lebanese regulatory requirements.

3.1 AI Governance Structure

3.1.1 AI Governance Committee

The establishment of a dedicated AI Governance Committee is fundamental to effective AI oversight within financial institutions. This committee serves as the central decision-making body for AI strategy, policy, and risk management, ensuring that AI initiatives align with business objectives and regulatory requirements.

Note for Lebanese Institutions: *For smaller institutions with limited resources, establishing a new standalone committee may not be feasible. Instead, an AI governance subcommittee can be formed under the existing Board Risk Committee or IT Steering Committee.*

Committee Composition: The AI Governance Committee should include senior representatives from key business and control functions [20]:

- **Chief Executive Officer or Deputy:** Provides executive leadership and strategic direction for AI initiatives.
- **Chief Risk Officer:** Ensures comprehensive risk management and regulatory compliance.
- **Chief Information Officer:** Provides technical expertise and infrastructure oversight.
- **Chief Data Officer:** Ensures data governance and quality management.
- **Chief Compliance Officer:** Ensures regulatory compliance and policy adherence.
- **Business Line Representatives:** Provide business context and use case expertise.
- **Legal Counsel:** Provides legal guidance and regulatory interpretation.
- **External AI Expert (Advisory):** Provides independent expertise and industry perspective.

Committee Responsibilities: The AI Governance Committee has broad responsibilities for AI oversight and governance [21]:

I. **Strategic Oversight:** The committee provides strategic direction for AI initiatives, ensuring alignment with business strategy, risk appetite, and regulatory requirements. This includes approving AI strategy documents, setting AI investment priorities, and establishing performance metrics for AI initiatives.

II. **Policy Development and Approval:** The committee is responsible for developing and approving comprehensive AI policies, including the Master AI Governance Policy, AI Risk Management Policy, AI Ethics Policy, and supporting procedures and standards.

III. **Risk Appetite Setting:** The committee establishes the institution's risk appetite for AI systems, including acceptable levels of model risk, operational risk, and compliance risk. This risk appetite guides decision-making throughout the AI lifecycle.

IV. **Resource Allocation:** The committee oversees resource allocation for AI initiatives, including budget approval, staffing decisions, and technology investments. This ensures that adequate resources are available for both AI development and governance activities.

V. **Performance Monitoring:** The committee monitors the performance of AI systems and governance processes, reviewing key metrics, incident reports, and audit findings. This includes regular assessment of AI system effectiveness, risk management performance, and compliance status.

VI. **Regulatory Engagement:** The committee oversees regulatory engagement related to AI systems, including approval submissions, regulatory reporting, and response to regulatory inquiries. Engage proactively with BDL for customer-facing or high-impact systems

3.1.2 AI Risk Management Office

The **AI Risk Management Office** serves as a specialized function within the second line of defense, providing dedicated expertise for **AI risk identification, assessment, and management**. This office works closely with the AI Governance Committee and business lines to ensure comprehensive risk oversight.

Office Structure and Staffing: The AI Risk Management Office should be staffed with professionals who possess both risk management expertise and technical knowledge of AI systems [22]:

- **AI Risk Manager:** Senior professional with expertise in both risk management and AI technologies.
- **Model Risk Specialists:** Professionals with expertise in model validation, testing, and monitoring.
- **Data Scientists:** Technical professionals who understand AI algorithms and can assess model performance.
- **Compliance Specialists:** Professionals with expertise in regulatory requirements and compliance monitoring.

Key Responsibilities:

I. **AI Risk Framework Development:** The office develops and maintains comprehensive risk management frameworks specifically designed for AI systems. This includes risk identification methodologies, assessment criteria, and mitigation strategies tailored to AI-specific risks.

II. **Model Validation and Testing:** The office oversees model validation activities, including performance testing, bias assessment, robustness testing, and ongoing monitoring. This ensures that AI models meet performance standards and regulatory requirements.

III. **Risk Assessment and Reporting:** The office conducts regular risk assessments of AI systems and provides comprehensive reporting to the AI Governance Committee and senior management. This includes risk dashboards, trend analysis, and recommendations for risk mitigation.

IV. **Incident Management:** The office manages AI-related incidents, including model failures, bias incidents, and security breaches. This includes incident investigation, root cause analysis, and implementation of corrective actions.

V. **Regulatory Compliance Monitoring:** The office monitors compliance with AI-related regulatory requirements and internal policies, conducting regular compliance assessments and reporting compliance status to relevant stakeholders.

3.2 Three Lines of Defense Model for AI

The Three Lines of Defense model provides a comprehensive framework for AI governance, ensuring clear roles and responsibilities across the organization while maintaining appropriate independence and oversight.

3.2.1 First Line of Defense: Business Lines and AI Development Teams

The first line of defense consists of business lines and AI development teams who are responsible for the day-to-day management and operation of AI systems. This line has primary responsibility for implementing AI governance requirements and managing AI-related risks.

Business Line Responsibilities:

I. **AI System Ownership:** Business lines serve as the primary owners of AI systems, with responsibility for defining business requirements, use cases, and success criteria. This includes maintaining clear documentation of AI system purpose, scope, and expected outcomes.

II. **Risk Identification and Management:** Business lines are responsible for identifying and managing AI-related risks within their areas of responsibility. This includes conducting initial risk assessments, implementing risk controls, and monitoring risk indicators.

III. **Policy Implementation:** Business lines must implement AI governance policies and procedures within their operations, ensuring that AI systems are developed, deployed, and operated in accordance with established standards.

IV. **Performance Monitoring:** Business lines monitor the performance of AI systems under their ownership, including tracking key performance indicators, identifying performance issues, and implementing corrective actions.

V. **User Training and Support:** Business lines provide training and support to end users of AI systems, ensuring that users understand system capabilities, limitations, and appropriate use cases.

AI Development Team Responsibilities:

I. **Technical Implementation:** AI development teams are responsible for the technical implementation of AI systems, including model development, testing, deployment, and maintenance. This includes following established development methodologies and quality standards.

II. **Documentation and Version Control:** Development teams maintain comprehensive documentation of AI systems, including technical specifications, model documentation, and change logs. This includes implementing robust version control for models, data, and code.

III. **Quality Assurance:** Development teams implement quality assurance processes throughout the AI development lifecycle, including code reviews, testing procedures, and validation activities.

IV. **Security Implementation:** Development teams implement security controls for AI systems, including access controls, encryption, and secure coding practices. This includes addressing AI-specific security risks such as adversarial attacks and data poisoning.

V. **Collaboration with Control Functions:** Development teams work closely with second- and third-line functions to ensure that governance requirements are properly implemented and that control functions have access to necessary information and systems.

3.2.2 Second Line of Defense: Risk Management and Compliance Functions

The second line of defense provides independent oversight and challenge of AI activities, ensuring that risks are properly identified, assessed, and managed. This line includes specialized AI risk management functions as well as traditional risk and compliance functions.

AI Risk Management Function:

I. **Independent Risk Assessment:** The AI risk management function conducts independent assessments of AI systems and related risks, providing objective evaluation of risk levels and control effectiveness.

II. **Model Validation:** This function oversees comprehensive model validation activities, including performance testing, bias assessment, robustness testing, and ongoing monitoring. Model validation ensures that AI systems meet performance standards and regulatory requirements.

III. **Risk Monitoring and Reporting:** The function implements comprehensive risk monitoring for AI systems, including real-time monitoring of model performance, drift detection, and anomaly identification. Regular risk reporting provides visibility into AI risk status and trends.

IV. **Policy Development and Maintenance:** The function develops and maintains AI risk management policies, procedures, and standards, ensuring that they remain current with evolving risks and regulatory requirements.

V. **Training and Awareness:** The function provides training and awareness programs for AI risks, ensuring that staff across the organization understand AI-related risks and their responsibilities for risk management.

Compliance Function:

I. **Regulatory Compliance Monitoring:** The compliance function monitors adherence to AI-related regulatory requirements, including BDL circulars, data protection laws, and other applicable regulations.

II. **Policy Compliance Assessment:** The function assesses compliance with internal AI governance policies and procedures, conducting regular compliance reviews and testing.

III. **Regulatory Reporting:** The function manages regulatory reporting related to AI systems, including preparation of regulatory submissions and response to regulatory inquiries.

IV. **Compliance Training:** The function provides compliance training related to AI governance, ensuring that staff understand regulatory requirements and compliance obligations.

V. **Issue Management:** The function manages compliance issues related to AI systems, including investigation of compliance breaches and implementation of corrective actions.

3.2.3 Third Line of Defense: Internal Audit

The third line of defense provides independent assurance on the effectiveness of AI governance, risk management, and compliance processes. Internal audit plays a critical role in ensuring that AI governance frameworks are operating effectively and that risks are being effectively managed.

Internal Audit Responsibilities:

I. **Governance Effectiveness Assessment:** Internal audit assesses the effectiveness of AI governance structures, including the AI Governance Committee, AI Risk Management Office, and related governance processes.

II. **Risk Management Audit:** Internal audit evaluates the effectiveness of AI risk management processes, including risk identification, assessment, monitoring, and mitigation activities.

III. **Compliance Audit:** Internal audit assesses compliance with AI-related regulatory requirements and internal policies, providing independent verification of compliance status.

IV. **Control Testing:** Internal audit tests the effectiveness of AI-related controls, including technical controls, process controls, and oversight controls.

V. **Model Validation Review:** Internal audit reviews model validation activities to ensure that they are comprehensive, independent, and effective in identifying model risks.

VI. **Audit Reporting:** Internal audit provides regular reporting on AI governance effectiveness, including audit findings, recommendations, and management responses.

Specialized AI Audit Capabilities:

Given the technical complexity of AI systems, internal audit functions should develop specialized capabilities for AI auditing [23]:

I. **Technical Expertise:** Audit teams should include professionals with technical expertise in AI systems, including data scientists, machine learning engineers, and AI specialists.

II. **AI Audit Methodologies:** Audit functions should develop specialized audit methodologies for AI systems, including techniques for testing model performance, assessing data quality, and evaluating algorithmic fairness.

III. **Continuous Auditing:** Given the dynamic nature of AI systems, audit functions should implement continuous auditing techniques that provide ongoing assurance rather than point-in-time assessments.

IV. **Collaboration with External Experts:** Audit functions should establish relationships with external AI experts who can provide specialized knowledge and independent perspectives on AI risks and controls.

3.3 AI Policy Framework

The AI policy framework provides the foundation for AI governance within financial institutions, establishing clear requirements, standards, and procedures for AI development, deployment, and operation.

3.3.1 Master AI Governance Policy

The Master AI Governance Policy serves as the overarching policy document that establishes the institution's approach to AI governance. This policy should be approved by the AI Governance Committee and reviewed regularly to ensure continued relevance and effectiveness.

Policy Scope and Objectives: The Master AI Governance Policy should clearly define its scope, covering all AI systems and related activities within the institution. The policy should establish clear objectives for AI governance, including:

- Ensuring safe and responsible AI development and deployment
- Managing AI-related risks effectively
- Maintaining compliance with regulatory requirements
- Promoting ethical AI practices
- Enabling innovation while maintaining appropriate controls

Governance Structure: The policy should clearly define the AI governance structure, including roles and responsibilities of the AI Governance Committee, AI Risk Management Office, and other key stakeholders.

Risk Management Framework: The policy should establish the overall framework for AI risk management, including risk appetite, risk categories, assessment methodologies, and mitigation strategies.

Compliance Requirements: The policy should specify compliance requirements for AI systems, including regulatory obligations, internal standards, and reporting requirements.

Ethical Principles: The policy should establish clear ethical principles for AI development and deployment, including commitments to fairness, transparency, accountability, and human oversight.

3.3.2 Supporting Policies and Procedures

The Master AI Governance Policy should be supported by detailed policies and procedures that address specific aspects of AI governance:

I. **AI Risk Management Policy:** This policy provides detailed guidance on AI risk management, including risk identification methodologies, assessment criteria, mitigation strategies, and monitoring requirements.

II. **AI Model Development Policy:** This policy establishes requirements for AI model development, including development methodologies, quality standards, testing requirements, and documentation standards.

III. **AI Data Governance Policy:** This policy addresses data governance requirements for AI systems, including data quality standards, privacy protections, and data lifecycle management.

IV. **AI Ethics Policy:** This policy establishes detailed requirements for ethical AI development and deployment, including bias prevention, fairness assessment, and transparency requirements.

V. **AI Incident Management Policy:** This policy provides procedures for managing AI-related incidents, including incident classification, response procedures, and reporting requirements.

VI. **AI Vendor Management Policy:** This policy addresses requirements for managing third-party AI vendors and services, including due diligence requirements, contract standards, and ongoing monitoring obligations.

3.3.3 Standards and Procedures

Detailed standards and procedures should be developed to support policy implementation:

I. **Technical Standards:** Technical standards should address AI system architecture, security requirements, performance standards, and integration requirements.

II. **Operational Procedures:** Operational procedures should provide step-by-step guidance for AI system deployment, monitoring, maintenance, and decommissioning.

III. **Quality Assurance Procedures:** Quality assurance procedures should establish requirements for testing, validation, and quality control throughout the AI lifecycle.

IV. **Documentation Standards:** Documentation standards should specify requirements for AI system documentation, including technical specifications, risk assessments, and operational procedures.

V. **Training and Awareness Procedures:** Training procedures should establish requirements for AI-related training and awareness programs for staff at all levels of the organization.

3.4 Human Oversight and Accountability

While AI systems can automate complex processes, ultimate accountability remains with the financial institution. Establishing a robust framework for meaningful human oversight is not only a best practice but a core requirement of international standards like the EU AI Act for high-risk systems. The objective is not to merely have a human in the loop, but to ensure that human intervention is effective, timely, and risk-informed.

3.4.1 Levels of Human Oversight

Institutions should classify AI systems to determine the required level of human oversight:

Human-in-the-Loop (HITL): Required for high-risk decisions. The AI system cannot proceed or finalize a decision without explicit human review and approval at a critical juncture. This is mandatory for processes such as final loan approvals, large-scale fraud alerts, or any action with significant, irreversible consequences for a customer.

Human-on-the-Loop (HOTL): Recommended for moderate-risk systems. The AI system operates autonomously, but a human operator continuously monitors its performance and can intervene or override its decisions at any time. This is suitable for algorithmic trading, real-time credit monitoring, or sophisticated AML transaction monitoring systems.

Human-in-Command (HIC): For low-risk automation. The AI system operates with a high degree of autonomy within a predefined scope. Human oversight is focused on monitoring overall system performance and outcomes, rather than individual decisions. This may apply to internal process automation or predictive maintenance.

3.4.2 Framework for Effective Oversight

An effective oversight framework must include the following components:

Clear Intervention Points: For HITL and HOTL systems, the points at which human intervention is possible or required must be clearly defined, documented, and designed into the system's workflow.

Override Authority & Escalation: Clear lines of authority must be established. Staff must know who has the authority to override an AI decision and what the escalation path is if they disagree with the AI's recommendation. These override actions must be logged and audited.

Informed Reviewer Principle: The human overseer must be equipped with sufficient information and understanding to make an informed judgment. This includes not only the AI's recommendation but also the key data and confidence scores that led to it. Interfaces must be designed for interpretability.

Training and Competency: Staff tasked with overseeing AI systems must receive specialized training on the model's capabilities, limitations, and common failure modes. They should be assessed for competency in their oversight role.

"Right to Challenge": Both employees and customers should have a clear and accessible process to challenge or request a review of a significant decision made by an AI system. This process must be handled by a human independent of the AI system's direct operation.

3.4.3 Prohibiting "Automation Bias"

Policies and training must actively seek to combat **automation bias,** the tendency for humans to over-rely on or place excessive trust in automated systems. Oversight personnel must be trained to maintain professional skepticism, question the AI's output, and not treat the model's recommendation as infallible. Performance reviews for these roles should reward critical thinking and appropriate challenges to the AI system, not just efficiency.

4. Cross-Framework Alignment and Gaps

4.1 International Standards Alignment

Lebanese financial institutions should align their AI governance frameworks with established international standards to ensure robustness and prepare for future regulatory developments. This alignment provides several benefits, including access to proven methodologies, enhanced credibility with stakeholders, and preparation for potential adoption of international standards by Lebanese regulators.

4.1.1 ISO/IEC 42001:2023 - AI Management Systems

ISO/IEC 42001:2023 provides a framework for establishing, implementing, maintaining, and continually improving AI management systems within organizations [13]. This standard is particularly relevant for financial institutions seeking to demonstrate systematic and responsible AI governance.

Key Requirements:

I. **Leadership and Commitment:** Senior management must demonstrate leadership and commitment to the AI management system

II. **AI Policy:** Organizations must establish and maintain an AI policy that reflects their commitment to responsible AI

III. **Risk Management:** Comprehensive risk management processes specifically designed for AI systems

IV. **Competence and Training:** Ensuring that personnel have appropriate competence for AI-related roles

V. **Documentation:** Maintaining comprehensive documentation of AI systems and processes

VI. **Monitoring and Review:** Regular monitoring and review of AI system performance and governance effectiveness

Implementation Considerations for Lebanese Institutions:

- Adapt ISO 42001 requirements to align with BDL regulatory expectations
- Integrate ISO 42001 processes with existing quality management systems
- Ensure documentation meets both ISO requirements and BDL approval processes
- Establish clear metrics for measuring AI management system effectiveness

4.1.2 EU AI Act Principles

While the EU AI Act does not directly apply to Lebanese institutions, its principles provide valuable guidance for responsible AI governance [3]. The Act's risk-based approach and emphasis on human oversight align well with prudent risk management practices.

Key Principles:

I. **Risk-Based Classification:** AI systems are classified based on their risk level, with higher-risk systems subject to more stringent requirements

II. **Human Oversight:** Meaningful human oversight is required for high-risk AI systems

III. **Transparency:** Users must be informed when they are interacting with AI systems

IV. **Accuracy and Robustness:** AI systems must be accurate, robust, and secure

V. **Data Governance:** High-quality data governance is essential for AI system performance

Adaptation for Lebanese Context:

- Apply risk-based classification to prioritize governance efforts
- Implement human oversight requirements aligned with BDL expectations
- Establish transparency requirements appropriate for Lebanese banking culture
- Develop data governance standards that comply with Lebanese data sovereignty requirements

4.1.3 NIST AI Risk Management Framework

The NIST AI Risk Management Framework (AI RMF 1.0) provides a comprehensive approach to managing AI risks throughout the AI lifecycle [4]. This framework is particularly valuable for its practical guidance and risk-based approach.

Framework Components:

A. **Govern:** Establish governance structures and processes for AI risk management

B. **Map:** Identify and categorize AI risks and their potential impacts

C. **Measure:** Develop metrics and methods for assessing AI risks

D. **Manage:** Implement controls and mitigation strategies for identified risks

Integration with Lebanese Requirements:

- Align NIST governance recommendations with BDL oversight expectations
- Adapt risk mapping techniques to address Lebanese regulatory requirements
- Develop measurement approaches that support BDL reporting requirements
- Implement management controls that address Lebanese operational context
- requirements

4.1.4 ISO/IEC 27001:2022 - The Foundation for Information Security

While ISO/IEC 42001 provides the framework for an AI Management System (AIMS), ISO/IEC 27001:2022 establishes the ISMS that secures the data, infrastructure, and

processes on which AI systems rely. The 2022 Annex A controls are grouped into Organizational (A.5), People (A.6), Physical (A.7), and Technological (A.8). For AI governance, critical areas include A.5 (governance, supplier/cloud security, threat intelligence), A.6 (competence and awareness for AI roles), A.7 (physical controls), and A.8 (secure development lifecycle A.8.25–A.8.29, access control, logging/monitoring, vulnerability management, cryptography, and data lifecycle controls). Effectiveness depends on applying Clauses 4–10 of ISO/IEC 27001, especially risk assessment/treatment and change control, so that AI-specific risks are systematically managed.

Key Annex A control areas relevant to AI:

- **A.5 Organizational Controls:** Governance, risk, threat intelligence (A.5.7), information security in project management (A.5.8), supplier relationships (A.5.19–A.5.22), information security for cloud services (A.5.23).
- **A.6 People Controls:** Screening, terms and conditions, awareness and training, disciplinary process, ensuring competence and conduct for AI developers and data handlers.
- **A.7 Physical Controls:** Facility and device protections affecting AI training/serving infrastructure.
- **A.8 Technological Controls:** Identity management (A.8.2), authentication information (A.8.3), access rights (A.8.4), privileged access rights (A.8.5), protection against malware (A.8.7), management of technical vulnerabilities (A.8.8), configuration management (A.8.9), information deletion (A.8.10), data masking (A.8.11), data leakage prevention (A.8.12), information classification (A.8.13), logging (A.8.15), monitoring (A.8.16), use of cryptography (A.8.24), and secure development (A.8.25–A.8.29), including secure architecture and engineering principles.

Note that Annex A is a reference set: per 27001:2022, controls in Annex A are selected based on risk treatment; they're not mandatory in full. Detailed implementation guidance for these controls is provided in ISO/IEC 27002:2022.

Management clause linkage for AI:

- Clause 4: Include AI-specific context and interested parties (e.g., regulators, data subjects).
- Clause 5: Commitment, roles, and policy (important for AIMS–ISMS alignment and accountability for AI risk owners).
- Note: Policy alignment includes model risk ownership and segregation of duties between model builders and validators.
- Clause 6: Extend risk assessment to AI risks (model misuse, data poisoning, prompt injection, model theft, output safety).
- Clause 7: Ensure competence and awareness for AI engineers and data scientists.
- Clause 8: Operationalize controls in MLOps/LLMOps pipelines (change management, deployment, rollback).

- Clause 9: Monitor AI-specific KPIs/KRIs (security incidents involving models, drift leading to security exposure).
- Clause 10: Continual improvement and corrective actions for AI-related incidents and post-mortems.

Note interplay with AI-specific standards:

- ISO/IEC 42001 (AIMS) complements 27001 by addressing AI-specific governance. Also relevant are ISO/IEC 23894 (AI risk management), ISO/IEC 27032/27036/27017/27018 (cybersecurity, supplier, and cloud/data protection), and ISO/IEC 27701 (PIMS), all commonly applicable in AI stacks. These supplier controls also apply to model providers, dataset vendors, and API-based AI services.

Aligning with ISO 27001 ensures that the foundational security posture of the institution is strong enough to support the unique risks introduced by AI.

4.2 Regulatory Gap Analysis

4.2.1 Current Regulatory Gaps

The absence of explicit AI regulations in Lebanon creates several gaps that institutions must address through interpretation and best practices:

Technical Standards Gap:

- No specific technical standards for AI systems in financial services
- Limited guidance on AI system architecture and security requirements
- Absence of model validation standards specific to AI systems

Risk Management Gap:

- No explicit AI risk management requirements
- Limited guidance on AI-specific risk categories and assessment methods
- Absence of AI risk appetite and tolerance frameworks

Governance Gap:

- No specific requirements for AI governance structures
- Limited guidance on AI oversight and decision-making processes
- Absence of AI-specific roles and responsibilities definitions

Compliance Gap:

- No explicit compliance requirements for AI systems
- Limited guidance on AI-related regulatory reporting
- Absence of AI-specific audit and assurance requirements

4.2.2 Gap Mitigation Strategies

Proactive Interpretation:

- Develop documented interpretations of existing regulations as they apply to AI systems
- Engage with BDL to seek guidance on AI-related regulatory expectations
- Participate in industry forums to develop common approaches to regulatory interpretation

International Best Practices Adoption:

- Selectively adopt relevant international standards and frameworks
- Adapt international practices to Lebanese regulatory context
- Maintain awareness of international regulatory developments

Industry Collaboration:

- Participate in industry associations and working groups focused on AI governance
- Share best practices and lessons learned with peer institutions
- Collaborate on common challenges and solutions

4.3 Future Regulatory Preparedness

4.3.1 Anticipated Regulatory Developments

Lebanese financial institutions should prepare for potential future regulatory developments in AI governance:

AI-Specific Regulations:

- BDL may issue specific circulars addressing AI systems in financial services
- Potential adoption or adaptation of international AI regulatory frameworks
- Development of Lebanese AI governance standards and requirements

Enhanced Data Protection:

- Strengthening of data protection requirements aligned with international standards
- Potential adoption of GDPR-like requirements for data processing
- Enhanced requirements for cross-border data transfers

Operational Resilience:

- Strengthened requirements for AI system resilience and business continuity
- Enhanced requirements for AI system monitoring and incident response
- Potential requirements for AI system testing and validation

4.3.2 Preparedness Strategies

Regulatory Monitoring:

- Establish processes for monitoring regulatory developments in AI governance
- Maintain awareness of international regulatory trends and their potential impact
- Engage with regulators and industry associations to stay informed of developments

Framework Flexibility:

- Design AI governance frameworks that can adapt to changing regulatory requirements
- Implement modular approaches that allow for easy updates and enhancements
- Maintain documentation that can support various regulatory reporting requirements

Capability Building:

- Develop internal capabilities for AI governance and risk management
- Invest in training and development for AI-related roles
- Build relationships with external experts and service providers

5. Technical Architecture and Security

5.1 AI System Architecture Principles

Foundational Note on ISO/IEC 27001:2022: The technical and security controls detailed in this section are not designed to exist in a vacuum. They should be implemented as part of a comprehensive Information Security Management System (ISMS), for which **ISO/IEC 27001:2022** is the international standard. An effective ISMS provides the governance, risk management, and control framework necessary to protect all information assets, including the data and models central to AI systems. The following guidance should be seen as an AI-specific application of the principles and controls defined within ISO 27001.

5.1.1 Security by Design

AI systems in Lebanese financial institutions must incorporate security considerations from the initial design phase, following the principle of "security by design" [27]. This approach ensures that security is not an afterthought but an integral part of the system architecture.

Core Security Principles:

A. **Least Privilege:** AI systems should operate with the minimum privileges necessary to perform their functions

B. **Defense in Depth:** Multiple layers of security controls should protect AI systems and data

C. **Fail Secure:** AI systems should fail in a secure state that protects sensitive data and operations

D. **Separation of Duties:** Critical AI operations should require multiple authorizations or validations

E. **Audit and Monitoring:** All AI system activities should be logged and monitored for security purposes

Implementation Considerations:

- Design AI system architectures that support granular access controls
- Implement network segmentation to isolate AI systems from other network resources
- Establish secure communication channels for AI system interactions
- Design audit logging that captures all relevant security events
- Implement real-time monitoring and alerting for security incidents

5.1.2 Data Sovereignty Compliance

Given Lebanese data sovereignty requirements, AI system architectures must carefully consider data residency, processing locations, and cross-border data flows [11].

Architectural Requirements:

I. **Local Data Processing:** Sensitive financial data should be processed within Lebanese jurisdiction

II. **Data Classification:** Clear classification of data types and their processing requirements

III. **Cross-Border Controls:** Technical controls to prevent unauthorized data transfers

IV. **Audit Trails:** Comprehensive logging of data access, processing, and movement

V. **Encryption:** Strong encryption for data at rest and in transit

Implementation Strategies:

- Deploy AI systems in Lebanese data centers or private cloud environments
- Implement data loss prevention (DLP) tools to monitor and control data movement
- Use encryption with keys managed within Lebanese jurisdiction
- Establish clear data flow documentation and approval processes
- Implement technical controls to enforce data residency requirements

5.1.3 Scalability and Performance

AI system architectures must support the scalability and performance requirements of financial services while maintaining security and compliance [28].

Scalability Considerations:

I. **Horizontal Scaling:** Design systems that can scale by adding additional resources

II. **Load Balancing:** Implement load balancing to distribute AI processing across multiple systems

III. **Caching:** Use caching strategies to improve AI system response times

IV. **Resource Management:** Implement dynamic resource allocation based on demand

V. **Performance Monitoring:** Continuous monitoring of system performance and capacity

Performance Optimization:

- Optimize AI model architectures for production deployment
- Implement model serving infrastructure that supports high-throughput requirements
- Use appropriate hardware acceleration (GPUs, TPUs) where beneficial
- Implement efficient data pipelines that minimize processing latency
- Establish performance baselines and monitoring thresholds

5.2 Infrastructure Security

5.2.1 Network Security

Network security for AI systems requires specialized considerations beyond traditional IT security measures [29].

Note for Lebanese Institutions*: When choosing between local cloud providers and on-premises infrastructure, institutions must weigh the data sovereignty benefits of local hosting against the potential resilience and scalability of reputable local cloud providers, while carefully considering local infrastructure reliability (e.g., power supply, internet connectivity).*

Network Architecture:

I. **Network Segmentation:** Isolate AI systems in dedicated network segments

II. **Micro-segmentation:** Implement granular network controls between AI system components

III. **Zero Trust Architecture:** Implement zero trust principles for AI system access

IV. **Network Monitoring:** Deploy specialized monitoring for AI system network traffic

V. **Intrusion Detection:** Implement AI-aware intrusion detection and prevention systems

Access Controls:

- Multi-factor authentication for all AI system access
- Role-based access controls aligned with AI governance roles
- Privileged access management for AI system administration
- Regular access reviews and certification processes
- Automated access provisioning and deprovisioning

5.2.2 Data Protection

Data protection for AI systems requires comprehensive controls throughout the data lifecycle [30].

Data Encryption:

I. **Encryption at Rest:** All AI training data and models should be encrypted when stored

II. **Encryption in Transit:** All data transfers should use strong encryption protocols

III. **Key Management:** Implement robust key management practices for AI system encryption

IV. **Tokenization:** Use tokenization to protect sensitive data in AI processing

V. **Format Preserving Encryption:** Use FPE where necessary to maintain data utility

Data Access Controls:

- Implement fine-grained access controls for AI training and inference data
- Use data masking and anonymization techniques where appropriate
- Establish clear data retention and disposal policies for AI systems
- Implement data loss prevention controls for AI system data
- Monitor and log all data access activities

5.2.3 Model Protection

AI models represent valuable intellectual property and must be protected from theft, tampering, and unauthorized access [31].

Model Security Measures:

I. **Model Encryption:** Encrypt AI models both at rest and during transmission

II. **Access Controls:** Implement strict access controls for AI model repositories

III. **Version Control:** Maintain secure version control for AI models with audit trails

IV. **Integrity Checking:** Implement integrity checking to detect model tampering

V. **Secure Deployment**: Use secure deployment processes that protect model confidentiality

Intellectual Property Protection:

- Implement legal and technical measures to protect proprietary AI models
- Use secure enclaves or trusted execution environments where appropriate
- Implement model obfuscation techniques to protect against reverse engineering
- Establish clear policies for model sharing and collaboration
- Monitor for unauthorized model access or extraction

5.3 AI-Specific Security Threats

5.3.1 Adversarial Attacks

Adversarial attacks represent a unique threat to AI systems, where malicious inputs are designed to cause AI systems to make incorrect decisions [32].

Types of Adversarial Attacks:

I. **Evasion Attacks:** Attacks designed to cause misclassification during inference

II. **Poisoning Attacks:** Attacks that corrupt training data to compromise model integrity

III. **Model Extraction:** Attacks designed to steal or reverse-engineer AI models

IV. **Membership Inference:** Attacks that determine whether specific data was used in training

V. **Property Inference:** Attacks that infer properties of training data

Defense Strategies:

- Implement adversarial training techniques to improve model robustness
- Use input validation and sanitization to detect malicious inputs
- Implement ensemble methods to reduce vulnerability to adversarial attacks
- Deploy anomaly detection systems to identify unusual input patterns
- Conduct regular adversarial testing of AI systems

5.3.2 Data Poisoning

Data poisoning attacks involve injecting malicious data into training datasets to compromise AI model integrity [33].

Poisoning Attack Types:

A. **Label Flipping:** Changing labels in training data to cause misclassification

B. **Feature Poisoning:** Modifying feature values to bias model behavior

C. **Backdoor Attacks:** Inserting triggers that cause specific malicious behaviors

D. **Availability Attacks:** Degrading overall model performance through poisoned data

Prevention and Detection:

- Implement data validation and quality checks for training data
- Use statistical methods to detect anomalous data points
- Implement data provenance tracking to verify data sources
- Use robust training algorithms that are resistant to poisoning
- Conduct regular model validation to detect performance degradation

5.3.3 Model Inversion and Extraction

These attacks attempt to extract sensitive information from AI models or steal the models themselves [34].

Attack Techniques:

A. **Model Inversion:** Reconstructing training data from model outputs

B. **Model Extraction:** Creating substitute models that mimic target model behavior

C. **Membership Inference:** Determining whether specific data was used in training

D. **Property Inference:** Inferring properties of the training dataset

Protection Measures:

- Implement differential privacy techniques in model training
- Use output perturbation to prevent precise model inversion
- Implement query limits and monitoring for model serving APIs
- Use secure multi-party computation for sensitive model operations
- Implement model watermarking to detect unauthorized copying

6. Data Governance and Privacy

6.1 Data Governance Framework for AI

6.1.1 Data Quality Management

High-quality data is essential for effective AI systems, and financial institutions must implement comprehensive data quality management processes [35].

Data Quality Dimensions:

I. **Accuracy:** Data should correctly represent the real-world entities or events it describes

II. **Completeness:** Data should be complete and not missing critical information

III. **Consistency:** Data should be consistent across different systems and time periods

IV. **Timeliness:** Data should be current and updated as needed for AI system requirements

V. **Validity:** Data should conform to defined formats, ranges, and business rules

VI. **Uniqueness:** Data should not contain inappropriate duplicates

Data Quality Processes:

A. **Data Profiling:** Regular analysis of data to understand its characteristics and quality

B. **Data Cleansing:** Processes to identify and correct data quality issues

C. **Data Validation:** Automated checks to ensure data meets quality standards

D. **Data Monitoring:** Ongoing monitoring of data quality metrics and trends

E. **Data Quality Reporting:** Regular reporting on data quality status and issues

Implementation for AI Systems:

- Establish data quality requirements specific to AI use cases
- Implement automated data quality checks in AI data pipelines
- Develop data quality metrics that align with AI model performance requirements
- Create feedback loops between model performance and data quality processes
- Establish data quality governance processes for AI training and inference data

6.1.2 Data Lineage and Provenance

Understanding the origin, transformation, and movement of data is critical for AI governance and regulatory compliance [36].

Data Lineage Components:

I. **Data Sources:** Identification of all data sources used in AI systems

II. **Data Transformations**: Documentation of all data processing and transformation steps

III. **Data Movement:** Tracking of data movement between systems and environments

IV. **Data Usage:** Documentation of how data is used in different AI systems and processes

V. **Data Dependencies:** Understanding of dependencies between different data elements

Implementation Requirements:

- Implement automated data lineage tracking tools
- Maintain comprehensive documentation of data flows and transformations
- Establish data lineage standards and documentation requirements
- Implement data lineage visualization tools for stakeholders
- Integrate data lineage information with AI model documentation

Regulatory Benefits:

- Support regulatory reporting and audit requirements
- Enable impact analysis for data changes and issues
- Facilitate compliance with data protection and privacy requirements
- Support model validation and risk assessment activities
- Enable effective incident response and root cause analysis

6.1.3 Data Classification and Handling

Proper data classification is essential for implementing appropriate security controls and ensuring compliance with regulatory requirements [37].

Data Classification Scheme:

A. **Public:** Data that can be freely shared without restriction

B. **Internal:** Data intended for internal use within the organization

C. **Confidential:** Sensitive data that requires protection from unauthorized disclosure

D. **Restricted:** Highly sensitive data with strict access and handling requirements

E. **Customer Data:** Personal and financial data belonging to customers

F. **Regulatory Data:** Data subject to specific regulatory requirements

Handling Requirements by Classification:

- Define specific handling requirements for each data classification level
- Implement technical controls to enforce data handling requirements
- Establish data retention and disposal requirements by classification
- Define access control requirements based on data classification
- Implement data loss prevention controls aligned with classification levels

AI-Specific Considerations:

- Classify AI training data based on sensitivity and regulatory requirements
- Implement controls for AI model outputs that may contain sensitive information
- Establish requirements for data anonymization and pseudonymization in AI systems
- Define data sharing requirements for AI development and testing activities
- Implement controls for AI system logs and audit data

6.2 Privacy Protection

6.2.1 Privacy by Design

Privacy by Design principles should be embedded in all AI systems from the initial design phase [38].

Core Principles:

I. **Proactive not Reactive:** Anticipate and prevent privacy invasions before they occur

II. **Privacy as the Default:** Maximum privacy protection without requiring action from the individual

III. **Full Functionality:** Accommodate all legitimate interests without unnecessary trade-offs

IV. **End-to-End Security:** Secure data throughout the entire lifecycle

V. **Visibility and Transparency:** Ensure all stakeholders can verify privacy practices

VI. **Respect for User Privacy:** Keep user interests paramount

Implementation in AI Systems:

- Design AI systems to minimize data collection and processing
- Implement privacy-preserving AI techniques such as differential privacy
- Use data minimization principles in AI model training and inference
- Implement user consent management systems for AI data processing
- Design AI systems with built-in privacy controls and user rights

6.2.2 Data Subject Rights

Lebanese financial institutions must implement processes to support data subject rights as required by Law 81/2018 and international best practices [12].

Key Data Subject Rights:

A. **Right of Access:** Individuals can request information about their data processing

B. **Right of Rectification:** Individuals can request correction of inaccurate data

C. **Right of Erasure:** Individuals can request deletion of their personal data

D. **Right of Portability:** Individuals can request their data in a portable format

E. **Right to Object:** Individuals can object to certain types of data processing

F. **Right to Restrict Processing:** Individuals can request limitation of data processing

Implementation for AI Systems:

- Design AI systems to support data subject rights requests
- Implement processes to identify and extract individual data from AI systems
- Establish procedures for correcting or deleting data in AI training datasets
- Develop capabilities to explain AI decision-making to data subjects
- Implement consent management systems for AI data processing
- Establish processes for handling data subject rights requests related to AI systems

6.2.3 Cross-Border Data Transfers

Given Lebanese data sovereignty requirements, cross-border data transfers for AI systems require careful consideration and control [11].

Transfer Requirements:

I. **Legal Basis:** Establish legal basis for cross-border data transfers

II. **Adequacy Decisions:** Verify adequacy of data protection in destination countries

III. **Safeguards:** Implement appropriate safeguards for data transfers

IV. **Data Mapping:** Maintain comprehensive mapping of cross-border data flows

V. **Transfer Agreements:** Establish appropriate contractual protections for data transfers

AI-Specific Considerations:

- Evaluate data transfer requirements for AI model training and inference
- Implement technical controls to prevent unauthorized data transfers
- Establish processes for approving AI-related cross-border data transfers
- Implement monitoring and logging of cross-border data movements
- Develop contingency plans for restrictions on cross-border data transfers

Technical Implementation:

- Use encryption and tokenization to protect data during transfers
- Implement data loss prevention controls for cross-border transfers
- Use secure communication channels for all data transfers
- Implement geographic restrictions on data processing and storage
- Monitor and log all cross-border data transfer activities

6.3 Consent Management

6.3.1 Consent Framework for AI

Obtaining and managing consent for AI data processing requires specialized approaches that address the unique characteristics of AI systems [39].

Consent Requirements:

I. **Informed Consent:** Individuals must understand how their data will be used in AI systems

II. **Specific Consent:** Consent must be specific to particular AI use cases and purposes

III. **Freely Given:** Consent must be given without coercion or negative consequences

IV. **Withdrawable:** Individuals must be able to withdraw consent at any time

V. **Granular Consent:** Consent should be granular enough to allow choice over different uses

AI-Specific Challenges:

- AI systems may use data for purposes not originally anticipated
- AI models may infer information not explicitly provided by individuals
- AI systems may combine data from multiple sources in complex ways
- AI decision-making processes may be difficult to explain to individuals
- AI systems may evolve and change over time, affecting original consent

Implementation Strategies:

- Implement dynamic consent management systems that can adapt to changing AI uses
- Use layered consent approaches that provide different levels of detail
- Implement consent dashboards that allow individuals to manage their preferences
- Establish processes for re-consent when AI systems change significantly
- Use privacy-preserving techniques to minimize the need for individual consent

6.3.2 Consent Technology Solutions

Technology solutions can help automate and streamline consent management for AI systems [40].

Consent Management Platforms:

- Centralized platforms for managing consent across all AI systems
- Integration with AI systems to enforce consent preferences
- Automated consent collection and validation processes
- Consent analytics and reporting capabilities
- Support for complex consent scenarios and preferences

Technical Features:

- Real-time consent verification and enforcement
- Consent preference synchronization across systems
- Automated consent renewal and re-consent processes

- Consent audit trails and compliance reporting
- Integration with privacy management tools and processes

Implementation Considerations:

- Select consent management platforms that support AI-specific requirements
- Integrate consent management with AI development and deployment processes
- Implement consent verification in AI data pipelines and processing systems
- Establish consent monitoring and compliance reporting processes
- Train staff on consent management requirements and procedures

7. Risk Management Framework

The AI Risk Management Framework provides a comprehensive approach to identifying, assessing, monitoring, and mitigating risks associated with artificial intelligence systems in Lebanese financial institutions. This framework builds upon traditional risk management principles while addressing the unique characteristics and challenges of AI technologies.

7.1 AI Risk Categories and Classification

7.1.1 Model Risk

Model risk represents one of the most significant categories of AI-related risk, encompassing the potential for adverse outcomes resulting from decisions based on incorrect or misused AI models [24]. This risk category is particularly relevant for financial institutions given their reliance on models for critical business decisions.

Model Development Risk: This subcategory includes risks arising from flawed model design, inappropriate algorithm selection, or inadequate model specification. Common sources of model development risk include:

- **Inappropriate Algorithm Selection:** Choosing algorithms that are not suitable for the specific use case or data characteristics.
- **Inadequate Feature Engineering:** Failing to identify relevant features or including irrelevant or biased features.
- **Poor Model Architecture:** Designing model architectures that are overly complex, insufficiently robust, or inappropriate for the intended use.
- **Insufficient Training Data:** Using training datasets that are too small, unrepresentative, or of poor quality.
- **Inadequate Validation:** Failing to properly validate model performance across different scenarios and conditions.

Model Implementation Risk: This subcategory encompasses risks arising from errors in model implementation, deployment, or integration with existing systems. Key sources include:

- **Coding Errors:** Programming mistakes that cause models to behave differently than intended.
- **Data Pipeline Errors:** Mistakes in data preprocessing, transformation, or feature engineering pipelines.
- **Integration Issues:** Problems arising from integrating AI models with existing banking systems and processes.
- **Version Control Problems:** Deploying incorrect model versions or failing to maintain proper version control.
- **Configuration Errors:** Incorrect model configuration or parameter settings in production environments.

Model Performance Risk: This subcategory includes risks related to model performance degradation, drift, or failure to meet performance expectations. Sources include:

- **Model Drift:** Changes in data patterns or relationships that cause model performance to degrade over time.
- **Concept Drift:** Changes in the underlying relationships between input variables and target outcomes.
- **Data Quality Degradation:** Deterioration in input data quality that affects model performance.
- **Overfitting:** Models that perform well on training data but poorly on new, unseen data.
- **Underfitting:** Models that fail to capture important patterns and relationships in the data.

7.1.2 Operational Risk

Operational risk in AI systems encompasses the risk of loss resulting from inadequate or failed internal processes, people, and systems, or from external events affecting AI operations [25].

System Availability Risk: This includes risks related to AI system downtime, performance degradation, or failure to meet service level requirements. Key considerations include:

- **Infrastructure Failures:** Hardware or software failures that affect AI system availability.
- **Scalability Issues:** Inability to handle increased load or transaction volumes.
- **Dependency Failures:** Failures in third-party services or systems that AI systems depend on.
- **Maintenance Windows:** Planned downtime for system maintenance or updates.
- **Disaster Recovery:** Ability to restore AI services following major disruptions.

Process Risk: This encompasses risks arising from inadequate or failed AI-related processes, including:

- **Change Management:** Inadequate processes for managing changes to AI systems.

- **Incident Management:** Poor processes for detecting, responding to, and resolving AI-related incidents.
- **Monitoring and Alerting:** Inadequate monitoring of AI system performance and health.
- **Documentation:** Poor documentation of AI systems, processes, and procedures.
- **Training and Competency:** Inadequate training of staff responsible for AI systems.

Human Error Risk: This includes risks arising from human mistakes in AI system operation, maintenance, or decision-making:

- **Configuration Errors:** Mistakes in system configuration or parameter settings.
- **Data Entry Errors:** Mistakes in data input or preprocessing.
- **Procedural Violations:** Failure to follow established procedures and protocols.
- **Inadequate Oversight:** Insufficient human oversight of AI system decisions and outputs.
- **Skills Gaps:** Lack of necessary skills or knowledge among AI system operators.

7.1.3 Compliance and Regulatory Risk

Compliance and regulatory risks encompass the risk of legal or regulatory sanctions, financial loss, or reputation damage arising from failure to comply with applicable laws, regulations, or supervisory requirements related to AI systems [26].

Regulatory Approval Risk: This includes risks related to obtaining and maintaining necessary regulatory approvals for AI systems:

- **Approval Delays:** Delays in obtaining BDL approval for AI systems that require regulatory approval.
- **Approval Conditions:** Conditions imposed by regulators that limit AI system functionality or increase costs.
- **Ongoing Compliance:** Risk of losing regulatory approval due to compliance failures.
- **Regulatory Changes:** Changes in regulatory requirements that affect existing AI systems.

Data Protection Risk: This encompasses risks related to compliance with data protection and privacy requirements:

- **Data Subject Rights:** Failure to properly implement data subject rights such as access, rectification, and erasure.
- **Consent Management:** Inadequate processes for obtaining and managing consent for AI data processing.
- **Cross-Border Transfers:** Compliance risks related to transferring data across borders for AI processing.
- **Data Minimization:** Failure to implement data minimization principles in AI systems.

- **Purpose Limitation:** Using AI systems for purposes beyond those for which consent was obtained.

Financial Services Regulation Risk: This includes risks related to compliance with financial services regulations as they apply to AI systems:

- **Consumer Protection:** Risks related to unfair treatment of customers through AI systems.
- **Market Conduct:** Compliance risks arising from the use of AI systems in trading, market-making, or other activities that could impact fair dealing, transparency, or market integrity.
- **Anti-Money Laundering:** Risks related to AI systems used for AML/CFT compliance.
- **Credit Risk Management:** Compliance risks related to AI systems used for credit decisions.
- **Operational Risk Management:** Regulatory requirements for operational risk management of AI systems.

7.1.4 Ethical and Reputational Risk

Ethical and reputational risk encompasses the potential for negative public perception, customer dissatisfaction, or stakeholder concerns arising from AI system behavior that is perceived as unfair, biased, or unethical [27].

Bias and Discrimination Risk: This includes risks related to AI systems producing biased or discriminatory outcomes:

- **Historical Bias:** Bias present in training data that reflects historical discrimination or unfair practices.
- **Representation Bias:** Bias arising from unrepresentative training data that does not adequately reflect the target population.
- **Measurement Bias:** Bias arising from systematic errors in data collection or measurement.
- **Algorithmic Bias:** Bias introduced by the algorithm itself or its implementation.
- **Feedback Loops:** Bias that is amplified over time through feedback loops in AI systems.

Transparency and Explainability Risk: This encompasses risks related to lack of transparency or explainability in AI systems:

- **Black Box Models:** Use of complex models that cannot be easily explained or interpreted.
- **Lack of Transparency:** Insufficient disclosure of AI system use to customers or stakeholders.
- **Inadequate Explanations:** Providing explanations that are incomplete, inaccurate, or difficult to understand.

- **Regulatory Requirements:** Failure to meet regulatory requirements for AI system transparency.
- **Customer Expectations:** Failure to meet customer expectations for explanation of AI-driven decisions.

Social Impact Risk: This includes risks related to broader social impacts of AI systems:

- **Job Displacement:** Negative impacts on employment due to AI automation.
- **Digital Divide:** Exacerbating inequalities through differential access to AI-enabled services.
- **Privacy Erosion:** Contributing to erosion of privacy through extensive data collection and analysis.
- **Social Manipulation:** Use of AI systems in ways that manipulate or exploit vulnerable populations.
- **Environmental Impact:** Environmental costs associated with AI system development and operation.

7.2 Risk Assessment Methodologies

7.2.1 Quantitative Risk Assessment

Quantitative risk assessment provides numerical estimates of AI-related risks, enabling more precise risk measurement and comparison across different AI systems and risk categories.

Model Performance Metrics: Quantitative assessment of model risk should include comprehensive performance metrics that capture different aspects of model behavior:

1- Accuracy Metrics: These metrics measure how often the model makes correct predictions:

- **Overall Accuracy:** Percentage of correct predictions across all classes.
- **Precision:** Percentage of positive predictions that are actually correct.
- **Recall (Sensitivity):** Percentage of actual positive cases that are correctly identified.
- **Specificity:** Percentage of actual negative cases that are correctly identified.
- **F1 Score:** Harmonic mean of precision and recall, providing a balanced measure.

2- Robustness Metrics: These metrics assess model stability and reliability:

- **Prediction Stability:** Consistency of model predictions across similar inputs.
- **Adversarial Robustness:** Model performance when subjected to adversarial attacks.
- **Data Quality Sensitivity:** Impact of data quality issues on model performance.

- **Feature Importance Stability:** Consistency of feature importance rankings across different datasets.
- **Cross-Validation Performance:** Model performance across different validation sets.

3- Fairness Metrics: These metrics quantify potential bias and discrimination in model outputs:

- **Demographic Parity:** Equal positive prediction rates across different demographic groups.
- **Equalized Odds:** Equal true positive and false positive rates across groups.
- **Calibration:** Consistency of prediction confidence across different groups.
- **Individual Fairness:** Similar predictions for similar individuals.
- **Counterfactual Fairness:** Predictions that would be the same in a counterfactual world without sensitive attributes.

4- Statistical Risk Measures: Quantitative risk assessment should employ statistical measures to quantify uncertainty and risk:

- **Value at Risk (VaR):** Adaptation of traditional VaR concepts to AI systems:
    - **Model VaR:** Maximum expected loss from model errors at a given confidence level.
    - **Performance VaR:** Worst-case model performance at a given confidence level.
    - **Operational VaR:** Maximum expected operational loss from AI system failures.
- **Expected Shortfall:** Average loss beyond the VaR threshold, providing insight into tail risks:
    - **Model Expected Shortfall:** Average loss from model errors beyond the VaR threshold.
    - **Operational Expected Shortfall:** Average operational loss beyond the VaR threshold.
- **Confidence Intervals: Statistical ranges that capture uncertainty in risk estimates:**
    - **Performance Confidence Intervals:** Ranges of expected model performance.
    - **Loss Confidence Intervals:** Ranges of expected losses from AI-related risks**.**
    - **Prediction Intervals:** Ranges of expected model predictions.

7.2.2 Qualitative Risk Assessment

Qualitative risk assessment provides structured approaches to evaluating AI risks that may be difficult to quantify numerically but are nonetheless important for comprehensive risk management.

Risk Scoring Frameworks: Qualitative risk assessment should employ structured scoring frameworks that provide consistent evaluation criteria:

- **Likelihood Assessment:** Evaluation of the probability that risk event will occur:
    - **Very Low (1):** risk event is highly unlikely to occur (less than 5% probability)
    - **Low (2):** risk event is unlikely to occur (5-25% probability)
    - **Medium (3):** risk event may occur (25-75% probability)
    - **High (4):** risk event is likely to occur (75-95% probability)
    - **Very High (5):** risk event is almost certain to occur (greater than 95% probability)
- **Impact Assessment:** Evaluation of the potential consequences if a risk occurs:
    - **Very Low (1):** Minimal impact on operations, reputation, or financial performance.
    - **Low (2):** Minor impact that can be easily managed with existing resources.
    - **Medium (3):** Moderate impact requiring additional resources or management attention.
    - **High (4):** Significant impact affecting business operations or strategic objectives.
    - **Very High (5):** Severe impact threatening business viability or regulatory standing.

Risk Matrix: Combination of likelihood and impact scores to determine overall risk level:

- **Low Risk (2-6):** Acceptable risk requiring routine monitoring.
- **Medium Risk (7-12):** Moderate risk requiring active management and mitigation.
- **High Risk (13-20):** Significant risk requiring immediate attention and comprehensive mitigation.
- **Critical Risk (21-25):** Unacceptable risk requiring immediate action or system shutdown.

- **Expert Judgment Processes:** Qualitative risk assessment should incorporate structured expert judgment processes:

    - **Delphi Method:** Structured communication technique that relies on a panel of experts to converge on complex issues:
    - **Expert Panel Selection:** Identification of experts with relevant AI and risk management expertise.
    - **Iterative Questioning:** Multiple rounds of questionnaires with feedback between rounds.
    - **Consensus Building:** Process for achieving consensus on risk assessments and mitigation strategies.
    - **Documentation:** Comprehensive documentation of expert opinions and reasoning.
- **Scenario Analysis:** Systematic exploration of potential future scenarios and their risk implications:
    - **Scenario Development:** Creation of plausible future scenarios affecting AI systems.
    - **Impact Assessment:** Evaluation of AI system performance and risk under different scenarios
    - **Stress Testing:** Assessment of AI system resilience under extreme scenarios.
    - **Contingency Planning:** Development of response plans for different scenario outcomes

7.2.3 Integrated Risk Assessment

Integrated risk assessment combines quantitative and qualitative approaches to provide comprehensive evaluation of AI-related risks.

Multi-Criteria Decision Analysis: Structured approach to evaluating AI risks across multiple criteria and stakeholder perspectives:

- **Criteria Definition:** Identification of relevant criteria for AI risk assessment:
    - **Technical Performance:** Model accuracy, robustness, and reliability.
    - **Business Impact:** Effect on business objectives and operations.
    - **Regulatory Compliance:** Adherence to regulatory requirements and expectations.
    - **Ethical Considerations:** Fairness, transparency, and social impact.
    - **Operational Feasibility:** Implementation and maintenance requirements.
- **Weight Assignment:** Determination of relative importance of different criteria:

  - **Stakeholder Input:** Gathering input from different stakeholders on criteria importance.
  - **Analytical Hierarchy Process:** Structured method for determining criteria weights.
  - **Sensitivity Analysis:** Assessment of how changes in weights affect risk rankings.
  - **Documentation:** Clear documentation of weighting rationale and assumptions.
- **Risk Aggregation:** Combination of individual risk assessments into overall risk scores:
  - **Weighted Scoring:** Calculation of overall risk scores using weighted criteria.
  - **Risk Ranking:** Ranking of AI systems or risk scenarios based on overall scores.
  - **Uncertainty Analysis:** Assessment of uncertainty in aggregated risk scores.
  - **Validation:** Validation of aggregated scores against expert judgment and historical data.

7.3 Risk Monitoring and Control

7.3.1 Continuous Monitoring Systems

Continuous monitoring systems provide real-time visibility into AI system performance and risk indicators, enabling proactive risk management and rapid response to emerging issues.

Performance Monitoring: Continuous tracking of AI system performance across multiple dimensions:

- **Real-Time Metrics:** Monitoring of key performance indicators in real-time:
  - **Prediction Accuracy:** Continuous tracking of model prediction accuracy.
  - **Response Time:** Monitoring of AI system response times and latency.
  - **Throughput:** Tracking of transaction volumes and processing capacity.
  - **Error Rates:** Monitoring of system errors and exceptions.
  - **Resource Utilization:** Tracking computational resource usage.
- **Drift Detection:** Automated detection of changes in data patterns or model performance:
  - **Statistical Process Control:** Use of control charts to detect performance drift.
  - **Distribution Monitoring:** Tracking changes in input data distributions.

  - **Concept Drift Detection:** Identification of changes in underlying relationships.
  - **Feature Drift Monitoring:** Tracking changes in individual feature distributions.
  - **Performance Degradation Alerts:** Automated alerts when performance falls below thresholds.
- **Anomaly Detection:** Identification of unusual patterns or behaviors in AI systems:
  - **Statistical Anomaly Detection:** Use of statistical methods to identify outliers.
  - **Machine Learning Anomaly Detection:** Use of ML algorithms to detect unusual patterns.
  - **Behavioral Analysis:** Monitoring of AI system behavior patterns.
  - **Input Validation:** Detection of unusual or potentially malicious inputs.
  - **Output Validation:** Identification of unusual or unexpected outputs.
- **Risk Indicator Monitoring:** Continuous tracking of key risk indicators specific to AI systems:
- **Leading Indicators:** Metrics that provide early warning of potential risk events:
  - **Data Quality Metrics:** Indicators of deteriorating data quality input.
  - **Model Complexity Metrics:** Measures of model complexity and interpretability.
  - **Change Frequency:** Rate of changes to AI systems and models.
  - **Training Data Age:** Time since last model retraining or data refresh.
  - **Validation Performance:** Performance on validation datasets over time.
- **Lagging Indicators:** Metrics that confirm that risk events have occurred:
  - **Incident Frequency:** Number and severity of AI-related incidents.
  - **Customer Complaints:** Complaints related to AI system decisions or behavior.
  - **Regulatory Issues:** Regulatory findings or concerns related to AI systems.
  - **Financial Losses:** Losses attributable to AI system failures or errors.
  - **Reputation Impact:** Negative publicity or reputation damage related to AI systems.

7.3.2 Control Implementation

Effective risk control requires implementation of comprehensive control measures throughout the AI lifecycle, from development through deployment and ongoing operation.

Preventive Controls: Controls designed to prevent risk events from occurring:

- **Development Controls: Controls implemented during AI system development:**
    - **Code Review:** Systematic review of AI system code by independent reviewers.
    - **Model Validation:** Comprehensive validation of AI models before deployment.
    - **Testing Protocols:** Rigorous testing of AI systems across multiple scenarios
    - **Documentation Standards:** Requirements for comprehensive system documentation
    - **Approval Processes:** Formal approval processes for AI system deployment

Operational Controls: Controls implemented during AI system operation:

- **Access Controls:** Restrictions on who can access and modify AI systems.
    - **Change Management:** Formal processes for managing changes to AI systems.
    - **Monitoring Systems:** Continuous monitoring of AI system performance and behavior.
    - **Backup and Recovery:** Procedures for backing up and recovering AI systems.
    - **Incident Response:** Procedures for responding to AI-related incidents.

Detective Controls: Controls designed to detect risk events when they occur:

- **Monitoring and Alerting: Systems for detecting and alerting on risk events:**
    - **Performance Monitoring:** Continuous monitoring of AI system performance.
    - **Anomaly Detection:** Automated detection of unusual system behavior.
    - **Threshold Alerts:** Alerts when key metrics exceed predefined thresholds.
    - **Trend Analysis:** Analysis of trends in AI system performance and behavior.
    - **Exception Reporting:** Reporting of exceptions and unusual events.
- **Audit and Review: Regular assessment of AI system controls and performance:**
    - **Internal Audit:** Independent assessment of AI system controls and governance
    - **Management Review:** Regular management review of AI system performance and risks
    - **Compliance Assessment:** Assessment of compliance with regulatory requirements and internal policies

- **Third-Party Review:** Independent assessment by external experts or auditors
- **Benchmarking:** Comparison of AI system performance against industry benchmarks

Corrective Controls: Controls designed to correct problems and prevent recurrence:

- **Incident Response: Procedures for responding to and resolving AI-related incidents:**
  - **Incident Classification:** Classification of incidents by severity and type
  - **Response Procedures:** Step-by-step procedures for incident response
  - **Root Cause Analysis:** Analysis to identify underlying causes of incidents.
  - **Corrective Actions:** Implementation of actions to address root causes.
  - **Lessons Learned:** Documentation and sharing of lessons learned from incidents.

Continuous Improvement: Processes for continuously improving AI systems and controls:

- **Performance Analysis:** Regular analysis of AI system performance and effectiveness
- **Control Effectiveness Assessment:** Assessment of the effectiveness of risk controls.
- **Process Improvement:** Identification and implementation of process improvements.
- **Technology Updates:** Regular updates to AI systems and supporting technology.
- **Training and Development:** Ongoing training and development of AI-related skills and knowledge

8. Operational Resilience

8.1 Business Continuity for AI Systems

8.1.1 AI System Criticality Assessment

Financial institutions must assess the criticality of AI systems to business operations and develop appropriate continuity plans [41].

Criticality Assessment Criteria:

I. **Business Impact:** Assessment of the impact of AI system failure on business operations

II. **Customer Impact:** Evaluation of the impact on customer services and experience

III. **Regulatory Impact:** Assessment of regulatory consequences of AI system failure

IV. **Financial Impact:** Evaluation of potential financial losses from AI system disruption

V. **Reputational Impact:** Assessment of potential reputational damage from AI system issues

Assessment Process:

- Conduct comprehensive business impact analysis for each AI system
- Classify AI systems based on criticality levels (Critical, Important, Standard)
- Document dependencies between AI systems and other business processes
- Identify single points of failure in AI system architectures
- Establish recovery time objectives (RTO) and recovery point objectives (RPO) for each system

Documentation Requirements:

- Maintain comprehensive inventory of AI systems and their criticality levels
- Document business processes that depend on AI systems
- Identify key stakeholders and their roles in AI system continuity
- Document escalation procedures for AI system incidents
- Maintain contact information for AI system support and recovery teams

8.1.2 Backup and Recovery Procedures

AI systems require specialized backup and recovery procedures that address the unique characteristics of AI models and data [42].

Backup Requirements:

A. **Model Backups:** Regular backups of AI models, including all versions and configurations

B. **Data Backups:** Comprehensive backups of training data, inference data, and system logs

C. **Configuration Backups:** Backups of system configurations, parameters, and settings

D. **Code Backups:** Backups of AI system code, scripts, and deployment configurations

E. **Documentation Backups:** Backups of system documentation, procedures, and runbooks

Recovery Procedures:

- Develop step-by-step recovery procedures for different types of AI system failures
- Establish recovery priorities based on system criticality and business impact
- Implement automated recovery procedures where possible
- Establish manual recovery procedures for complex failure scenarios
- Document recovery testing procedures and schedules

Testing and Validation:

- Conduct regular testing of backup and recovery procedures
- Validate recovery procedures through simulated failure scenarios
- Test recovery time objectives and recovery point objectives
- Document test results and identify areas for improvement
- Update recovery procedures based on test results and lessons learned

8.1.3 Alternative Processing Arrangements

Financial institutions should establish alternative processing arrangements for critical AI systems.

Alternative Processing Options:

- **Hot Standby:** Fully operational backup systems that can take over immediately
- **Warm Standby:** Partially operational backup systems that can be activated quickly
- **Cold Standby:** Backup systems that require manual activation and configuration
- **Cloud Failover:** Cloud-based backup systems that can provide alternative processing
- **Manual Processes:** Manual procedures that can substitute for AI system functions

Implementation Considerations:

- Evaluate alternative processing options based on system criticality and cost
- Implement appropriate alternative processing arrangements for each AI system
- Test alternative processing arrangements regularly
- Train staff on alternative processing procedures
- Document alternative processing capabilities and limitations

8.2 Incident Management

8.2.1 AI Incident Classification

AI systems can experience unique types of incidents that require specialized classification and response procedures.

AI Incident Categories:

- **Model Performance Incidents:** Degradation in AI model accuracy or performance
- **Data Quality Incidents:** Issues with data quality that affect AI system performance

- **Bias and Fairness Incidents:** Discovery of bias or unfair treatment in AI system outputs
- **Security Incidents:** Cybersecurity incidents affecting AI systems or data
- **Compliance Incidents:** Violations of regulatory requirements or internal policies
- **Operational Incidents:** System failures, outages, or performance issues

Incident Severity Levels:

- **Critical:** Incidents that pose immediate risk to customers, operations, or compliance
- **High:** Incidents that have significant impact but do not pose immediate risk
- **Medium:** Incidents that have moderate impact and can be resolved within normal timeframes
- **Low:** Incidents that have minimal impact and can be resolved through routine procedures

Classification Criteria:

- Define specific criteria for classifying AI incidents by category and severity
- Establish clear escalation thresholds based on incident classification
- Document incident classification procedures and decision trees
- Train incident response teams on AI incident classification
- Regularly review and update incident classification criteria

8.2.2 Incident Response Procedures

AI incidents require specialized response procedures that address the technical and business complexities of AI systems.

Incident Response Team:

- **Incident Commander:** Overall responsibility for incident response coordination
- **Technical Lead:** Technical expertise for AI system troubleshooting and resolution
- **Business Lead:** Business expertise for impact assessment and stakeholder communication
- **Compliance Lead:** Compliance expertise for regulatory reporting and requirements
- **Communications Lead:** Responsibility for internal and external communications

Response Procedures:

1. **Detection and Alerting**: Automated and manual procedures for detecting AI incidents
2. **Initial Assessment:** Rapid assessment of incident scope, impact, and severity
3. **Containment:** Immediate actions to contain the incident and prevent further impact
4. **Investigation:** Detailed investigation to determine root cause and contributing factors
5. **Resolution:** Implementation of corrective actions to resolve the incident

6. **Recovery:** Restoration of normal AI system operations and validation of resolution
7. **Post-Incident Review:** Comprehensive review to identify lessons learned and improvements

Documentation Requirements:

- Maintain detailed incident logs and documentation
- Document all response actions and decisions
- Capture lessons learned and improvement opportunities
- Prepare incident reports for management and regulators
- Update incident response procedures based on lessons learned

8.2.3 Regulatory Reporting

AI incidents may require reporting to BDL and other regulators, depending on their nature and impact.

Reporting Requirements:

A. **Immediate Notification:** Immediate notification for critical incidents affecting customers or operations
B. **Detailed Reports:** Comprehensive incident reports within specified timeframes
C. **Follow-up Reports:** Regular updates on incident resolution and corrective actions
D. **Root Cause Analysis**: Detailed analysis of incident causes and contributing factors
E. **Corrective Action Plans:** Plans for addressing root causes and preventing recurrence

Reporting Considerations:

- Establish clear criteria for determining when regulatory reporting is required
- Develop templates and procedures for regulatory incident reporting
- Ensure incident reports address regulatory concerns and requirements
- Coordinate with legal and compliance teams on regulatory reporting
- Maintain records of all regulatory communications and responses

8.3 Change Management

8.3.1 AI System Change Control

Changes to AI systems require specialized change control procedures that address the unique risks and complexities of AI technologies.

Change Categories:

- **Model Changes:** Updates to AI models, algorithms, or parameters
- **Data Changes:** Changes to training data, data sources, or data processing
- **Infrastructure Changes:** Changes to AI system infrastructure or platforms

- **Configuration Changes:** Changes to system configurations or settings
- **Process Changes:** Changes to AI system processes or procedures

Change Control Process:

1. **Change Request:** Formal request for changes with business justification
2. **Impact Assessment:** Assessment of potential impacts and risks of proposed changes
3. **Approval Process:** Formal approval process based on change risk and impact
4. **Testing and Validation:** Comprehensive testing of changes before implementation
5. **Implementation:** Controlled implementation of approved changes
6. **Validation:** Post-implementation validation to ensure changes work as expected
7. **Documentation:** Complete documentation of changes and their impacts

Risk Assessment:

- Evaluate potential risks of proposed changes to AI systems
- Assess impact on model performance, accuracy, and fairness
- Evaluate compliance and regulatory implications of changes
- Consider operational and business impacts of changes
- Document risk assessment results and mitigation strategies

8.3.2 Model Versioning and Deployment

AI models require specialized versioning and deployment procedures to ensure traceability and control.

Model Versioning:

- **Version Control:** Comprehensive version control for all AI models and related artifacts
- **Metadata Management:** Detailed metadata for each model version including performance metrics
- **Lineage Tracking:** Complete lineage tracking from training data through model deployment
- **Rollback Capabilities:** Ability to rollback to previous model versions if needed
- **Archive Management:** Long-term archival of model versions for compliance and audit

Deployment Procedures:

1. **Staging Environment:** Comprehensive testing in staging environments before production deployment
2. **Gradual Rollout:** Gradual rollout procedures to minimize risk of deployment issues
3. **Monitoring and Validation:** Intensive monitoring during and after model deployment
4. **Rollback Procedures:** Rapid rollback procedures if deployment issues are identified

5. **Documentation:** Complete documentation of deployment procedures and results

Quality Assurance:

- Implement comprehensive quality assurance procedures for model deployment
- Conduct thorough testing of model performance and functionality
- Validate model behavior in production environments
- Monitor model performance after deployment
- Document quality assurance results and any issues identified

9. Third-Party Management

9.1 AI Vendor Risk Management

9.1.1 Vendor Due Diligence

Financial institutions must conduct comprehensive due diligence on AI vendors to ensure they meet regulatory requirements and risk management standards.

Due Diligence Components:

A. **Financial Stability:** Assessment of vendor financial health and business viability

B. **Technical Capabilities:** Evaluation of vendor technical expertise and AI capabilities

C. **Security Practices:** Review of vendor cybersecurity practices and controls

D. **Compliance Framework:** Assessment of vendor compliance with relevant regulations

E. **Data Governance:** Evaluation of vendor data governance and privacy practices

F. B**usiness Continuity:** Review of vendor business continuity and disaster recovery capabilities

Assessment Process:

1. Develop comprehensive vendor assessment questionnaires
2. Conduct on-site visits and technical reviews where appropriate
3. Review vendor certifications and third-party assessments
4. Evaluate vendor references and client testimonials
5. Conduct pilot projects or proof-of-concept implementations
6. Document assessment results and risk ratings

Documentation Requirements:

- Maintain comprehensive vendor assessment documentation
- Document vendor risk ratings and approval decisions

- Keep records of vendor certifications and compliance evidence
- Maintain vendor contact information and escalation procedures
- Document vendor performance metrics and service level agreements

9.1.2 Contractual Requirements

Contracts with AI vendors must include specific provisions to address AI-related risks and regulatory requirements.

Key Contractual Provisions:

A. **Service Level Agreements:** Clear SLAs for AI system performance and availability

B. **Data Protection:** Comprehensive data protection and privacy requirements

C. **Security Requirements:** Detailed cybersecurity requirements and controls

D. **Compliance Obligations:** Vendor obligations to comply with relevant regulations

E. **Audit Rights:** Rights to audit vendor practices and controls

F. **Liability and Indemnification:** Clear allocation of liability for AI system issues

G. **Termination Rights:** Rights to terminate contracts for cause or convenience

H. **Data Return and Destruction:** Requirements for data return and secure destruction

AI-Specific Considerations:

- Model performance guarantees and remedies for performance failures
- Intellectual property rights and protections for AI models and data
- Requirements for model explainability and transparency
- Obligations to address bias and fairness in AI systems
- Requirements for model validation and testing
- Provisions for regulatory reporting and cooperation

Contract Management:

- Establish contract management processes for AI vendor agreements
- Monitor vendor compliance with contractual obligations
- Conduct regular contract reviews and updates
- Manage contract renewals and renegotiations
- Document contract performance and any issues

9.1.3 Ongoing Monitoring

Continuous monitoring of AI vendors is essential to ensure ongoing compliance and performance.

Monitoring Activities:

- **Performance Monitoring:** Regular monitoring of vendor performance against SLAs
- **Security Monitoring:** Ongoing assessment of vendor security practices and incidents
- **Compliance Monitoring:** Regular review of vendor compliance with regulatory requirements
- **Financial Monitoring:** Ongoing assessment of vendor financial health and stability
- **Service Quality Monitoring:** Regular assessment of service quality and customer satisfaction
- **Risk Assessment Updates:** Periodic updates to vendor risk assessments

Monitoring Tools and Processes:

- Implement automated monitoring tools where possible
- Establish regular vendor review meetings and reporting
- Conduct periodic vendor assessments and audits
- Monitor vendor security incidents and responses
- Track vendor performance metrics and trends
- Maintain vendor scorecards and performance dashboards

Escalation and Remediation:

- Establish clear escalation procedures for vendor issues
- Define remediation requirements for vendor performance failures
- Implement vendor improvement plans where needed
- Consider contract termination for persistent vendor issues
- Document all vendor issues and remediation efforts

9.2 Cloud Service Providers

9.2.1 Cloud Security Requirements

AI systems deployed in cloud environments require additional security considerations and controls.

Cloud Security Framework:

A. **Shared Responsibility Model:** Clear understanding of security responsibilities between institution and cloud provider

B. **Data Sovereignty:** Ensuring data remains within Lebanese jurisdiction as required

C. **Access Controls:** Comprehensive access controls for cloud-based AI systems

D. **Encryption:** Strong encryption for data at rest and in transit in cloud environments

E. **Network Security:** Secure network configurations and monitoring in cloud environments

F. **Incident Response:** Coordinated incident response procedures with cloud providers

Implementation Requirements:

1. Select cloud providers that meet Lebanese data sovereignty requirements
2. Implement cloud security controls aligned with BDL Circular 144/2017
3. Establish cloud monitoring and logging procedures
4. Implement cloud access management and authentication controls
5. Conduct regular cloud security assessments and audits
6. Maintain cloud security documentation and procedures

Compliance Considerations:

1. Ensure **data protection and customer information privacy** requirements comply with BDL Circular 146/2018
2. Implement controls to meet data protection requirements
3. Establish procedures for regulatory reporting of cloud incidents
4. Maintain audit trails for cloud-based AI system activities
5. Document cloud security controls and compliance measures

9.2.2 Data Residency and Sovereignty

Cloud-based AI systems must comply with Lebanese data sovereignty requirements [11], recommending contractual data residency commitments, key management in-country, and audit rights for geo-controls.

Data Residency Requirements:

A. **Local Data Storage:** Sensitive financial data must be stored within Lebanese jurisdiction

B. **Processing Locations:** AI processing of sensitive data should occur within Lebanon

C. **Data Transfer Controls:** Technical controls to prevent unauthorized cross-border data transfers

D. **Backup and Recovery:** Backup and recovery systems must comply with data residency requirements

E. **Audit and Monitoring:** Comprehensive monitoring of data location and movement

Implementation Strategies:

1. Select cloud providers with data centers in Lebanon or approved jurisdictions
2. Implement technical controls to enforce data residency requirements
3. Use encryption and tokenization to protect data in cloud environments
4. Establish data classification and handling procedures for cloud deployments
5. Monitor and log all data access and movement activities

Compliance Validation:

1. Conduct regular audits of data residency compliance
2. Implement automated monitoring of data location and movement
3. Maintain documentation of data residency controls and procedures
4. Report data residency compliance to regulators as required
5. Address any data residency violations promptly and thoroughly

9.2.3 Service Level Agreements

Cloud service agreements for AI systems require specific SLAs that address AI-related requirements.

AI-Specific SLAs:

- **Model Performance:** SLAs for AI model accuracy, latency, and throughput
- **Data Availability:** SLAs for training and inference data availability
- **System Uptime:** SLAs for AI system availability and uptime
- **Support Response:** SLAs for technical support and issue resolution
- **Security Incident Response:** SLAs for security incident detection and response
- **Compliance Reporting:** SLAs for compliance reporting and documentation

Monitoring and Enforcement:

1. Implement monitoring tools to track SLA compliance
2. Establish regular SLA reporting and review processes
3. Define penalties and remedies for SLA violations
4. Conduct periodic SLA reviews and updates
5. Document SLA performance and any issues

9.3 AI Model Providers

9.3.1 Model Validation Requirements

Third-party AI models require comprehensive validation to ensure they meet performance and risk requirements.

Validation Components:

A. **Performance Validation:** Testing of model accuracy, precision, recall, and other performance metrics

B. **Robustness Testing:** Testing of model performance under various conditions and scenarios

C. **Bias Assessment:** Testing for bias and fairness in model outputs

D. **Security Testing:** Testing for vulnerabilities to adversarial attacks and other security threats

E. **Compliance Validation:** Ensuring models comply with regulatory requirements

F. **Documentation Review:** Review of model documentation and technical specifications

Validation Process:

1. Develop comprehensive model validation procedures
2. Conduct independent validation using institution's own data and scenarios
3. Compare model performance against benchmarks and alternatives
4. Test model behavior in production-like environments
5. Document validation results and any issues identified
6. Obtain validation sign-off from appropriate stakeholders

Ongoing Validation:

- Implement ongoing monitoring of model performance
- Conduct periodic re-validation of models
- Monitor for model drift and degradation
- Update validation procedures based on experience and lessons learned
- Document ongoing validation activities and results

9.3.2 Model Documentation

Third-party AI models must be accompanied by comprehensive documentation that supports governance and risk management.

Required Documentation:

A. **Model Description:** Detailed description of model purpose, functionality, and use cases

B. **Technical Specifications:** Technical details of model architecture, algorithms, and parameters

C. **Training Data:** Information about training data sources, quality, and characteristics

D. **Performance Metrics:** Detailed performance metrics and validation results

E. **Limitations and Risks:** Documentation of model limitations and associated risks

F. **Usage Guidelines:** Guidelines for appropriate model usage and deployment

G. **Maintenance Requirements:** Requirements for model maintenance and updates

Documentation Standards:

- Establish documentation standards for third-party AI models
- Require vendors to provide documentation in specified formats
- Review documentation for completeness and accuracy
- Maintain documentation repositories for all AI models

- Update documentation as models are modified or updated

Documentation Review:

- Conduct thorough review of model documentation before deployment
- Validate documentation accuracy through testing and validation
- Identify any gaps or deficiencies in documentation
- Require vendors to address documentation issues
- Maintain documentation review records and approvals

9.3.3 Intellectual Property Considerations

Use of third-party AI models raises important intellectual property considerations that must be addressed.

IP Risk Assessment:

A. **Ownership Rights:** Clear understanding of model ownership and usage rights

B. **License Terms:** Comprehensive review of license terms and restrictions

C. **Derivative Works:** Understanding of rights to modify or enhance models

D. **Confidentiality:** Protection of proprietary model information and trade secrets

E. **Indemnification:** Protection against IP infringement claims

F. **Termination Rights:** Rights and obligations upon contract termination

IP Protection Measures:

- Implement technical measures to protect third-party IP
- Establish access controls for proprietary models and information
- Train staff on IP protection requirements and obligations
- Monitor for unauthorized use or disclosure of third-party IP
- Maintain records of IP licenses and usage rights

IP Compliance:

- Ensure compliance with all IP license terms and restrictions
- Monitor for changes in IP ownership or licensing terms
- Address any IP compliance issues promptly
- Maintain documentation of IP compliance efforts
- Report IP issues to legal and compliance teams as appropriate

10. AML/CFT and Special Considerations

10.1 AI in Anti-Money Laundering

10.1.1 AML Model Governance

AI systems used for Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) require specialized governance due to their regulatory importance and complexity [43].

AML AI Governance Framework:

A. **Specialized Oversight:** Dedicated governance for AML AI systems within the broader AI governance framework

B. **Regulatory Alignment:** Alignment with AML/CFT regulatory requirements and expectations

C. **Model Validation:** Comprehensive validation procedures for AML AI models

D. **Performance Monitoring:** Continuous monitoring of AML AI system performance and effectiveness

E. **Documentation Standards:** Enhanced documentation requirements for AML AI systems

F. **Audit and Review:** Regular audit and review of AML AI systems and controls

Key Governance Considerations:

- AML AI systems must maintain high levels of accuracy to minimize false positives and negatives
- Model explainability is crucial for regulatory reporting and investigation support
- Data quality is critical for effective AML detection and investigation
- Model bias could lead to discriminatory monitoring or investigation practices
- System availability is essential for continuous transaction monitoring
- Integration with existing AML processes and systems is required

Regulatory Requirements:

- Ensure AML AI systems comply with BDL AML/CFT requirements
- Maintain audit trails for all AML AI system decisions and actions
- Provide explanations for AML AI system alerts and decisions
- Support regulatory examinations and inquiries related to AML AI systems
- Report AML AI system issues and incidents to appropriate authorities
- Maintain AML AI system documentation for regulatory review

10.1.2 Transaction Monitoring Systems

AI-powered transaction monitoring systems require specialized considerations for effectiveness and compliance [44].

System Design Considerations:

1. **Real-time Processing:** Ability to process transactions in real-time or near real-time
2. **Scalability:** Ability to handle high transaction volumes and peak loads
3. **Accuracy:** High accuracy to minimize false positives while maintaining detection effectiveness
4. **Explainability:** Ability to explain alerts and decisions for investigation and reporting
5. **Integration:** Integration with existing AML systems and processes
6. **Flexibility:** Ability to adapt to changing money laundering typologies and methods

Model Development:

- Use diverse and representative training data that reflects current money laundering methods
- Implement ensemble methods to improve detection accuracy and reduce false positives
- Incorporate domain expertise and regulatory guidance in model development
- Test models against known money laundering scenarios and typologies
- Validate model performance using independent datasets and scenarios
- Document model development processes and decisions

Operational Considerations:

- Establish clear procedures for alert investigation and case management
- Train investigators on AI-generated alerts and their interpretation
- Implement quality assurance procedures for alert investigation and disposition
- Monitor system performance and effectiveness metrics
- Conduct regular model updates and retraining based on new data and typologies
- Maintain comprehensive audit trails for all system activities

10.1.3 Customer Due Diligence Enhancement

AI can enhance Customer Due Diligence (CDD) processes while requiring careful governance and oversight.

AI Applications in CDD:

1. **Identity Verification:** AI-powered identity verification and document authentication
2. **Risk Assessment:** AI-based customer risk scoring and classification

3. **Adverse Media Screening:** AI-powered screening of adverse media and sanctions lists
4. **Beneficial Ownership Analysis:** AI-assisted analysis of complex ownership structures
5. **Ongoing Monitoring:** AI-powered ongoing monitoring of customer activities and risk profiles
6. **Enhanced Due Diligence:** AI-supported enhanced due diligence for high-risk customers

Implementation Requirements:

- Ensure AI-enhanced CDD processes comply with regulatory requirements
- Maintain human oversight and decision-making authority for CDD determinations
- Implement quality assurance procedures for AI-generated CDD information
- Provide training for staff on AI-enhanced CDD processes and tools
- Maintain audit trails for all AI-supported CDD activities and decisions
- Document AI-enhanced CDD procedures and controls

Risk Management:

- Address potential bias in AI-based risk assessment and customer classification
- Ensure AI systems do not discriminate against protected classes or groups
- Implement controls to prevent over-reliance on AI-generated CDD information
- Monitor AI system performance and accuracy in CDD applications
- Establish procedures for handling AI system errors or failures in CDD processes
- Maintain backup manual procedures for critical CDD functions

10.2 Regulatory Technology (RegTech)

10.2.1 Compliance Monitoring

AI-powered compliance monitoring systems can enhance regulatory compliance while requiring appropriate governance [45].

AI Applications in Compliance:

1. **Regulatory Change Management:** AI-powered monitoring of regulatory changes and updates
2. **Policy Compliance Monitoring:** AI-based monitoring of compliance with internal policies
3. **Regulatory Reporting:** AI-assisted preparation and validation of regulatory reports
4. **Examination Preparation:** AI-powered analysis and preparation for regulatory examinations

5. **Issue Identification:** AI-based identification of potential compliance issues and violations
6. **Training and Awareness:** AI-enhanced compliance training and awareness programs

Implementation Considerations:

- Ensure AI compliance systems are aligned with regulatory requirements and expectations
- Maintain human oversight and validation of AI-generated compliance information
- Implement quality assurance procedures for AI-supported compliance activities
- Provide training for compliance staff on AI-powered tools and systems
- Maintain comprehensive documentation of AI compliance system decisions and actions
- Establish procedures for handling AI system errors or failures in compliance monitoring

Governance Requirements:

- Include AI compliance systems in the overall AI governance framework
- Conduct regular validation and testing of AI compliance system accuracy and effectiveness
- Monitor AI compliance system performance and identify areas for improvement
- Maintain audit trails for all AI compliance system activities and decisions
- Report AI compliance system issues and incidents to appropriate stakeholders
- Conduct regular reviews of AI compliance system controls and procedures

10.2.2 Regulatory Reporting

AI can enhance regulatory reporting processes while requiring careful validation and oversight.

AI Applications in Reporting:

1. **Data Collection and Aggregation:** AI-powered collection and aggregation of regulatory reporting data
2. **Report Generation:** AI-assisted generation of regulatory reports and filings
3. **Data Quality Assurance:** AI-based validation of regulatory reporting data quality
4. **Exception Identification:** AI-powered identification of reporting exceptions and issues
5. **Trend Analysis:** AI-based analysis of regulatory reporting trends and patterns
6. **Submission Management:** AI-enhanced management of regulatory report submissions

Quality Assurance:

- Implement comprehensive quality assurance procedures for AI-generated regulatory reports
- Maintain human review and approval of all regulatory reports before submission
- Conduct regular validation of AI reporting system accuracy and completeness
- Monitor AI reporting system performance and identify areas for improvement
- Maintain backup manual procedures for critical regulatory reporting functions
- Document all AI reporting system controls and procedures

Regulatory Considerations:

- Ensure AI-generated regulatory reports meet all regulatory requirements and standards
- Maintain audit trails for all AI reporting system activities and decisions
- Provide explanations for AI-generated regulatory reporting data and calculations
- Support regulatory examinations and inquiries related to AI reporting systems
- Report AI reporting system issues and incidents to appropriate regulators
- Maintain AI reporting system documentation for regulatory review

10.3 Market Risk and Trading

10.3.1 Algorithmic Trading Governance

AI-powered algorithmic trading systems require specialized governance due to their potential market impact and regulatory requirements.

Governance Framework:

1. **Trading Algorithm Oversight:** Specialized oversight committee for AI trading algorithms
2. **Risk Management:** Comprehensive risk management framework for AI trading systems
3. **Market Impact Assessment:** Assessment of potential market impact of AI trading algorithms
4. **Regulatory Compliance:** Compliance with market conduct and trading regulations
5. **Performance Monitoring:** Continuous monitoring of AI trading system performance
6. **Incident Management:** Specialized incident management procedures for trading system issues

Risk Controls:

1. **Position Limits:** Automated position limits and risk controls for AI trading systems

2. **Market Risk Limits:** Real-time monitoring and enforcement of market risk limits
3. **Liquidity Controls:** Controls to ensure adequate liquidity for AI trading activities
4. **Circuit Breakers:** Automated circuit breakers to halt trading in abnormal market conditions
5. **Human Oversight:** Meaningful human oversight and intervention capabilities
6. **Kill Switches:** Emergency procedures to immediately halt AI trading activities

Regulatory Requirements:

- Ensure AI trading systems comply with market conduct regulations
- Maintain audit trails for all AI trading system decisions and activities
- Provide explanations for AI trading system behavior and decisions
- Report AI trading system issues and incidents to market regulators
- Support regulatory examinations and inquiries related to AI trading systems
- Maintain AI trading system documentation for regulatory review

10.3.2 Market Data and Analytics

AI systems used for market data analysis and investment decision-making require appropriate governance and controls.

Data Governance:

1. **Data Quality:** Ensure high-quality market data for AI analysis and decision-making
2. **Data Sources:** Validate and monitor market data sources and feeds
3. **Data Lineage:** Maintain comprehensive lineage tracking for market data
4. **Data Security:** Implement strong security controls for sensitive market data
5. **Data Retention:** Establish appropriate retention policies for market data and analysis
6. **Data Access:** Control access to market data based on business need and authorization

Model Validation:

- Conduct comprehensive validation of AI models used for market analysis
- Test model performance across different market conditions and scenarios
- Validate model assumptions and limitations
- Monitor model performance and accuracy over time
- Conduct regular model reviews and updates
- Document model validation activities and results

Investment Decision Support:

- Ensure AI-generated investment recommendations are properly validated and reviewed
- Maintain human oversight and decision-making authority for investment decisions
- Implement quality assurance procedures for AI-supported investment analysis
- Monitor AI system performance in investment decision support
- Maintain audit trails for AI-supported investment decisions
- Document AI investment decision support procedures and controls

10.4 Special Considerations for Generative AI

The rapid adoption of Generative AI (GenAI), including Large Language Models (LLMs), presents a unique and complex set of risks and opportunities that demand a specialized governance approach. Unlike traditional AI models that are predictive, GenAI models are creative, generating novel content (text, images, code) that can be difficult to verify and control. Financial institutions must establish clear policies and robust technical controls to manage their use.

10.4.1 Unique Risks of Generative AI

AI-powered algorithmic trading systems require specialized governance due to their potential market impact and regulatory requirements.

Governing GenAI requires understanding risks that are distinct from those of predictive AI:

A) Factual Hallucination: The model generates plausible but incorrect or fabricated information. In a financial context, this could lead to incorrect financial advice, flawed market analysis, or misleading customer communications.

Possible Mitigation:

1. Implement Retrieval-Augmented Generation (RAG) to ground responses in verified internal documents.
2. Require human verification for all externally-facing or decision-critical outputs.
3. Use fact-checking APIs and cross-referencing against trusted data sources.

B) Data Leakage & Privacy: Employees may inadvertently paste confidential customer or proprietary data into public GenAI tools, leading to data breaches and violations of the Banking Secrecy Law.

Possible Mitigation:

1. Prohibit the use of public GenAI tools (e.g., public versions of ChatGPT, Claude) with any non-public institutional or customer data.
2. Deploy private, sandboxed instances of LLMs within the institution's secure environment.

3. Implement data loss prevention (DLP) tools to monitor and block sensitive data in prompts.

C) Prompt Injection & Jailbreaking: Malicious actors can manipulate model inputs (prompts) to bypass safety controls, extract sensitive information from the model's context, or cause it to perform unauthorized actions.

Possible Mitigation:

1. Implement strict input validation and sanitization for all prompts, especially those from external users (e.g., in a customer-facing chatbot).
2. Use instruction-tuned models that are more resilient to adversarial prompts.
3. Maintain a library of known attack patterns and continuously test models against them.

D) Copyright & Intellectual Property: The model may generate content that infringes on existing copyrights, or the ownership of model-generated content may be legally ambiguous.

Possible Mitigation:

1. Use models from reputable providers who offer IP indemnification.
2. Establish clear policies on the ownership and use of AI-generated content.
3. Avoid using GenAI for creating public-facing marketing content without a thorough legal review.

E) Toxicity & Bias Amplification: GenAI models trained on vast, unvetted internet data can generate toxic, biased, or reputationally damaging content, amplifying societal biases at scale.

Possible Mitigation:

1. Implement robust output filters to detect and block harmful content.
2. Regularly audit model outputs for hidden biases related to gender, ethnicity, or other protected characteristics.
3. Fine-tune models on curated, high-quality internal data to align their outputs with institutional values.

10.4.2 Acceptable Use Policy (AUP) for Generative AI

All institutions must implement a mandatory AUP for all employees. This policy should be a prerequisite for accessing any GenAI tools and should clearly define:

- **Prohibited Data:** An explicit list of data types that must **never** be entered into public GenAI tools, including but not limited to: Customer Personally Identifiable Information (PII), financial records, non-public institutional data, trade secrets, and internal communications.

- **Approved Tools:** A definitive list of institution-approved GenAI tools and platforms. Access to any other tool must be explicitly forbidden.

- **Verification Requirements:** A mandate that any AI-generated information used for decision-making or external communication must be independently verified for accuracy by a qualified human expert.

- **Disclosure Rules:** Clear guidelines on when and how employees must disclose the use of AI in their work, both internally and to clients.

10.4.3 Technical Governance for Enterprise GenAI

For institution-sanctioned GenAI applications, the following technical controls are suggested:

- **Private Deployment:** Whenever possible, deploy models in a private cloud or on-premise environment to ensure data never leaves the institution's control, in line with data sovereignty principles.

- **Retrieval-Augmented Generation (RAG):** For internal knowledge management or customer support applications, use RAG architecture. This approach connects the LLM to a curated, internal knowledge base (e.g., policy documents, product specifications), forcing the model to generate answers based on this verified information rather than its internal, unvetted knowledge. This dramatically reduces hallucinations and ensures answers are aligned with institutional facts.

- **Monitoring and Logging:** All prompts and model responses must be logged for audit, security monitoring, and compliance purposes. This is critical for investigating incidents and demonstrating regulatory compliance.

11. Implementation Roadmap

The implementation of a comprehensive AI governance framework requires a structured, phased approach that balances the need for robust controls with the practical realities of organizational change and resource constraints. This roadmap provides a detailed timeline and methodology for implementing AI governance in Lebanese financial institutions.

11.1 Implementation Phases Overview

The AI governance implementation is structured into four distinct phases, each building upon the previous phase and designed to achieve specific milestones while maintaining operational continuity.

Phase 1: Foundation and Assessment (Months 1-6)

Objective: Establish the foundational elements of AI governance and conduct comprehensive assessment of current state.

Key Deliverables:

- AI Governance Committee establishment
- Current state assessment and gap analysis - Initial policy framework development
- Regulatory engagement initiation
- Resource allocation and team formation

Phase 2: Framework Development and Pilot Implementation (Months 7-12)

Objective: Develop comprehensive governance framework and implement pilot programs to test and refine approaches.

Key Deliverables:

- Complete policy and procedure development
- Risk management framework implementation.
- Pilot AI system governance implementation
- Staff training and capability building
- Technology infrastructure development

Phase 3: Full Implementation and Integration (Months 13-18)

Objective: Roll out governance framework across all AI systems and integrate with existing risk management and compliance processes.

Key Deliverables:

- Full governance framework deployment
- All AI systems under governance framework
- Integrated monitoring and reporting systems
- Comprehensive staff training completion
- Regulatory approval processes completion

Phase 4: Optimization and Continuous Improvement (Months 19-24)

Objective: Optimize governance processes based on experience and establish continuous improvement mechanisms.

Key Deliverables:

- Process optimization and refinement - Advanced analytics and monitoring implementation.
- Continuous improvement processes establishment

- Industry best practice adoption - Future roadmap development

11.2 Phase 1: Foundation and Assessment (Months 1-6)

11.2.1 Governance Structure Establishment

AI Governance Committee Formation (Month 1-2):

The establishment of the AI Governance Committee represents the critical first step in implementing effective AI governance. This committee will provide strategic oversight and decision-making authority for all AI-related initiatives within the institution.

Committee Charter Development: The committee charter should clearly define the committee's purpose, scope, authority, and operating procedures [28]. Key elements include:

- **Mission Statement:** Clear articulation of the committee's role in overseeing AI governance and ensuring responsible AI development and deployment.
- **Scope of Authority:** Definition of the committee's decision-making authority, including approval thresholds, escalation procedures, and reporting relationships.
- **Membership Criteria:** Specification of required skills, experience, and organizational representation for committee members.
- **Meeting Frequency:** Regular meeting schedule with provisions for emergency meetings when required.
- **Reporting Requirements:** Clear requirements for committee reporting to the board of directors and senior management.

Member Selection and Appointment: Committee members should be selected based on their expertise, organizational role, and ability to contribute to effective AI governance [29]. The selection process should include:

- **Skills Assessment:** Evaluation of candidates' technical knowledge, risk management experience, and governance expertise.
- **Organizational Representation:** Ensuring appropriate representation from key business lines and control functions.
- **Independence Considerations:** Balancing the need for business expertise with appropriate independence and objectivity.
- **Term Limits:** Establishing appropriate term limits to ensure fresh perspectives while maintaining continuity.
- **Training Requirements:** Identifying training needs for committee members to ensure they have necessary AI governance knowledge.

Operating Procedures Development: The committee should establish clear operating procedures that ensure effective and efficient decision-making [30]. These procedures should address:

- **Meeting Management:** Procedures for scheduling, conducting, and documenting committee meetings.

- **Decision-Making Processes:** Clear processes for making decisions, including voting procedures and consensus-building approaches.
- **Information Requirements:** Specification of information needed for effective decision-making, including reporting formats and data requirements.
- **Conflict of Interest Management:** Procedures for identifying and managing potential conflicts of interest among committee members.
- **Communication Protocols:** Clear protocols for communicating committee decisions and recommendations to relevant stakeholders.

AI Risk Management Office Establishment (Month 2-3):

The AI Risk Management Office serves as the specialized function responsible for day-to-day AI risk management activities and provides technical expertise to support the AI Governance Committee.

Office Structure Design: The office structure should be designed to provide comprehensive coverage of AI risk management activities while maintaining appropriate independence and objectivity [31]. Key considerations include:

- **Organizational Placement:** Positioning the office within the risk management function to ensure appropriate independence from AI development activities.
- **Reporting Relationships:** Clear reporting lines to the Chief Risk Officer and AI Governance Committee.
- **Staffing Requirements:** Determination of staffing levels and skill requirements based on the institution's AI portfolio and risk profile.
- **Budget Allocation:** Adequate budget allocation for staff, technology, and external expertise as needed.
- **Performance Metrics:** Establishment of clear performance metrics and objectives for the office.

Staff Recruitment and Training: The office should be staffed with professionals who possess both risk management expertise and technical knowledge of AI systems [32]. Recruitment and training activities should include:

- **Role Definition:** Clear definition of roles and responsibilities for office staff, including required skills and experience.
- **Recruitment Strategy:** Comprehensive recruitment strategy that may include internal transfers, external hiring, and contractor engagement.
- **Training Programs:** Comprehensive training programs to ensure staff have necessary AI risk management knowledge and skills.
- **Certification Requirements:** Consideration of relevant professional certifications for AI risk management.
- **Ongoing Development:** Plans for ongoing professional development and skill enhancement.

11.2.2 Current State Assessment

AI System Inventory (Month 1-4):

A comprehensive inventory of existing AI systems is essential for understanding the current state and establishing baseline governance requirements.

System Identification: The inventory process should identify all AI systems currently in use or under development within the institution [33]. This includes:

- **Customer-Facing Systems:** AI systems that directly interact with customers, such as chatbots, recommendation engines, and automated decision-making systems.
- **Internal Operations Systems:** AI systems used for internal operations, such as fraud detection, risk assessment, and process automation.
- **Third-Party Systems:** AI systems provided by external vendors or service providers.
- **Development Projects:** AI systems currently under development or in pilot phases.
- **Legacy Systems:** Older systems that may incorporate AI or machine learning capabilities.

System Classification: Each identified system should be classified based on its risk profile, business criticality, and regulatory impact [34]. Classification criteria should include:

- **Risk Level:** Assessment of the potential risk posed by the system based on its use case, data sensitivity, and decision-making authority.
- **Business Criticality:** Evaluation of the system's importance to business operations and the potential impact of system failure.
- **Regulatory Impact:** Assessment of whether the system falls under specific regulatory requirements or approval processes.
- **Data Sensitivity:** Evaluation of the types and sensitivity of data processed by the system.
- **Customer Impact:** Assessment of the system's direct or indirect impact on customers.

Documentation Requirements: For each identified system, comprehensive documentation should be collected or developed [35]. This documentation should include:

- **Technical Specifications:** Detailed technical documentation including system architecture, algorithms used, and integration points.
- **Business Requirements:** Clear documentation of business requirements, use cases, and success criteria.
- **Risk Assessments:** Existing risk assessments or identification of need for new risk assessments.
- **Compliance Documentation:** Documentation of compliance with existing policies and regulatory requirements.
- **Operational Procedures:** Documentation of operational procedures for system monitoring, maintenance, and support.

Gap Analysis (Month 3-5):

The gap analysis identifies differences between current AI governance practices and the requirements of the proposed governance framework.

Governance Gap Assessment: Evaluation of existing governance structures and processes compared to the proposed AI governance framework [36]. This assessment should cover:

- **Organizational Structure:** Comparison of existing governance structures with the proposed AI governance framework.
- **Policy Framework:** Assessment of existing policies and procedures against the requirements of comprehensive AI governance.
- **Risk Management:** Evaluation of current risk management practices for AI systems.
- **Compliance Processes:** Assessment of existing compliance processes and their adequacy for AI governance.
- **Monitoring and Reporting:** Evaluation of current monitoring and reporting capabilities for AI systems.

Technical Gap Assessment: Evaluation of existing technical capabilities and infrastructure against the requirements for effective AI governance [37]. This assessment should include:

- **Monitoring Capabilities:** Assessment of current capabilities for monitoring AI system performance and behavior.
- **Data Management:** Evaluation of data management capabilities including data quality, lineage, and governance.
- **Security Controls:** Assessment of existing security controls and their adequacy for AI systems.
- **Integration Capabilities:** Evaluation of capabilities for integrating AI governance tools with existing systems.
- **Reporting Infrastructure:** Assessment of current reporting infrastructure and its ability to support AI governance requirements.

Resource Gap Assessment: Evaluation of current resources (human, financial, and technological) against the requirements for implementing comprehensive AI governance [38]. This assessment should cover:

- **Staffing Requirements:** Assessment of current staffing levels and skills against the requirements for AI governance.
- **Budget Requirements:** Evaluation of financial resources needed for AI governance implementation.
- **Technology Requirements:** Assessment of technology infrastructure needs for AI governance.
- **Training Requirements:** Identification of training needs for existing staff.
- **External Support Requirements:** Assessment of needs for external expertise or support services.

11.2.3 Initial Policy Development

Master AI Governance Policy (Month 4-6):

The Master AI Governance Policy serves as the foundational document that establishes the institution's approach to AI governance and provides the framework for all other AI-related policies and procedures.

Policy Scope Definition: The policy scope should clearly define what is covered by the AI governance framework [39]. Key scope considerations include:

- **System Coverage:** Clear definition of which systems and technologies are considered AI systems subject to the governance framework.
- **Organizational Coverage:** Specification of which organizational units and functions are subject to AI governance requirements.
- **Activity Coverage:** Definition of which activities related to AI development, deployment, and operation are covered by the policy.
- **Third-Party Coverage:** Clarification of how the policy applies to third-party AI systems and services.
- **Exemptions:** Clear specification of any exemptions or special considerations for certain types of AI systems or activities.

Governance Principles: The policy should establish clear governance principles that guide all AI-related activities [40]. These principles should include:

- **Accountability:** Clear assignment of accountability for AI systems and their outcomes.
- **Transparency:** Commitment to transparency in AI system development, deployment, and operation.
- **Fairness:** Commitment to developing and deploying AI systems that are fair and non-discriminatory.
- **Human Oversight:** Requirement for meaningful human oversight of AI system decisions and operations.
- **Risk Management:** Commitment to comprehensive risk management throughout the AI lifecycle.
- **Compliance:** Commitment to compliance with all applicable laws, regulations, and internal policies.

Roles and Responsibilities: The policy should clearly define roles and responsibilities for AI governance [41]. This should include:

- **AI Governance Committee:** Clear definition of the committee's roles, responsibilities, and authority.
- **AI Risk Management Office:** Specification of the office's responsibilities and reporting relationships.

- **Business Lines:** Definition of business line responsibilities for AI systems under their ownership.
- **Control Functions:** Clarification of roles and responsibilities for risk management, compliance, and audit functions.
- **Individual Responsibilities:** Specification of individual responsibilities for staff involved in AI activities.

11.3 Phase 2: Framework Development and Pilot Implementation (Months 7-12)

11.3.1 Comprehensive Policy Framework Development

Supporting Policy Development (Month 7-9):

Building upon the Master AI Governance Policy, comprehensive supporting policies must be developed to address specific aspects of AI governance in detail.

AI Risk Management Policy: This policy provides detailed guidance on identifying, assessing, and managing AI-related risks [42]. Key components include:

- **Risk Categories:** Comprehensive definition of AI risk categories including model risk, operational risk, compliance risk, and reputational risk.
- **Risk Assessment Methodologies:** Detailed methodologies for conducting quantitative and qualitative risk assessments of AI systems.
- **Risk Appetite Framework:** Clear definition of the institution's risk appetite for different types of AI risks.
- **Risk Mitigation Strategies:** Comprehensive guidance on risk mitigation strategies and controls for different risk categories.
- **Risk Monitoring Requirements:** Detailed requirements for ongoing risk monitoring and reporting.

AI Model Development Policy: This policy establishes requirements and standards for AI model development activities. Essential elements include:

- **Development Methodologies:** Specification of approved methodologies for AI model development including agile, waterfall, and hybrid approaches.
- **Quality Standards:** Clear quality standards for AI models including performance, robustness, and reliability requirements.
- **Testing Requirements:** Comprehensive testing requirements including unit testing, integration testing, and user acceptance testing.
- **Documentation Standards:** Detailed documentation requirements for AI models including technical specifications, validation reports, and user guides.
- **Version Control:** Requirements for version control and change management for AI models and related artifacts.

AI Data Governance Policy: This policy addresses data governance requirements specific to AI systems. Critical components include:

- **Data Quality Standards:** Clear standards for data quality including accuracy, completeness, consistency, and timeliness requirements.
- **Data Lineage Requirements:** Requirements for tracking data lineage throughout the AI lifecycle.
- **Privacy Protection:** Detailed requirements for protecting personal data in AI systems including anonymization and pseudonymization techniques.
- **Data Retention:** Clear policies for data retention and disposal in AI systems.
- **Data Access Controls:** Requirements for controlling access to AI training and operational data.

Pilot Program Implementation (Month 8-11):

Pilot programs provide an opportunity to test and refine the AI governance framework before full implementation across all AI systems.

Pilot System Selection: The selection of pilot systems should be based on criteria that provide meaningful testing of the governance framework while managing implementation risk. Selection criteria should include:

- **Representative Use Cases:** Selection of systems that represent different types of AI use cases within the institution.
- **Risk Profile Diversity:** Including systems with different risk profiles to test risk management approaches.
- **Business Criticality:** Balancing the need for meaningful testing with the risk of disrupting critical business operations.
- **Technical Complexity:** Including systems with different levels of technical complexity to test governance scalability.
- **Stakeholder Engagement:** Selecting systems that involve different stakeholder groups to test governance processes.

Pilot Implementation Process: The pilot implementation should follow a structured process that enables systematic testing and refinement of governance approaches. Key process elements include:

- **Baseline Assessment:** Comprehensive assessment of pilot systems before governance implementation.
- **Governance Implementation:** Systematic implementation of governance framework components for pilot systems
- **Performance Monitoring:** Continuous monitoring of both system performance and governance process effectiveness.
- **Stakeholder Feedback:** Regular collection of feedback from stakeholders involved in pilot implementation.
- **Issue Identification:** Systematic identification and documentation of issues and challenges encountered during pilot implementation.

Lessons Learned Capture: The pilot program should include systematic capture and analysis of lessons learned to inform full implementation. This should include:

- **Process Effectiveness:** Assessment of the effectiveness of different governance processes and procedures.
- **Resource Requirements:** Evaluation of actual resource requirements compared to initial estimates.
- **Stakeholder Acceptance:** Assessment of stakeholder acceptance and engagement with governance processes.
- **Technical Challenges:** Identification of technical challenges and solutions for governance implementation.
- **Improvement Opportunities:** Identification of opportunities for improving governance processes and procedures.

11.3.2 Technology Infrastructure Development

Monitoring and Reporting Systems (Month 9-12):

Effective AI governance requires robust technology infrastructure to support monitoring, reporting, and control activities.

Monitoring Platform Selection: The selection of monitoring platforms should be based on comprehensive evaluation of available options against specific requirements. Key evaluation criteria include:

- **Functional Requirements:** Ability to monitor AI system performance, data quality, and risk indicators.
- **Integration Capabilities:** Ability to integrate with existing AI systems and infrastructure.
- **Scalability:** Ability to scale to support the institution's current and future AI portfolio.
- **Usability:** Ease of use for different types of users including technical and business stakeholders
- **Cost Considerations:** Total cost of ownership including licensing, implementation, and ongoing maintenance costs.

Dashboard Development: Comprehensive dashboards should be developed to provide visibility into AI system performance and governance metrics. Dashboard requirements include:

- **Executive Dashboards:** High-level dashboards for senior management and the AI Governance Committee.
- **Operational Dashboards:** Detailed dashboards for operational staff responsible for AI system management.
- **Risk Dashboards:** Specialized dashboards for risk management staff focusing on AI risk indicators.

- **Compliance Dashboards:** Dashboards for compliance staff focusing on regulatory and policy compliance metrics.
- **Technical Dashboards:** Detailed technical dashboards for AI development and operations teams.

Reporting Automation: Automated reporting capabilities should be implemented to ensure consistent and timely reporting of AI governance metrics. Automation requirements include:

- **Scheduled Reports:** Automated generation and distribution of regular governance reports.
- **Exception Reports:** Automated generation of reports when specific thresholds or conditions are met.
- **Regulatory Reports:** Automated preparation of reports required for regulatory submissions.
- **Trend Analysis:** Automated analysis and reporting of trends in AI system performance and governance metrics.
- **Alert Systems:** Automated alert systems for critical issues or threshold breaches.

11.4 Phase 3: Full Implementation and Integration (Months 13-18)

11.4.1 Framework Rollout

Systematic Rollout Process (Month 13-16):

The rollout of the AI governance framework across all AI systems requires careful planning and execution to ensure successful implementation while maintaining operational continuity.

Rollout Prioritization: AI systems should be prioritized for governance implementation based on risk profile, business criticality, and implementation complexity. Prioritization criteria include:

- **High-Risk Systems First:** Priority implementation for systems with high-risk profiles or significant regulatory impact.
- **Business Critical Systems:** Early implementation of systems that are critical to business operations.
- **Customer-Facing Systems:** Priority for systems that directly impact customers or require regulatory approval.
- **Implementation Complexity:** Consideration of implementation complexity and resource requirements.
- **Stakeholder Readiness:** Assessment of stakeholder readiness and capability for governance implementation.

Implementation Teams: Dedicated implementation teams should be established to manage the rollout process. Team structure should include:

- **Program Management:** Overall program management and coordination across different implementation streams.
- **Technical Implementation:** Technical teams responsible for implementing governance tools and processes.
- **Change Management:** Change management specialists to support organizational adoption of new processes.
- **Training and Support:** Teams responsible for providing training and ongoing support to users.
- **Quality Assurance:** Quality assurance teams to ensure proper implementation of governance requirements.

Progress Monitoring: Comprehensive progress monitoring should be implemented to track rollout progress and identify issues early. Monitoring should include:

- **Implementation Milestones:** Tracking of key implementation milestones and deliverables.
- **Resource Utilization:** Monitoring of resource utilization against planned budgets and timelines.
- **Issue Tracking:** Systematic tracking and resolution of implementation issues and challenges.
- **Stakeholder Feedback:** Regular collection and analysis of stakeholder feedback on implementation progress.
- **Quality Metrics:** Monitoring quality metrics to ensure proper implementation of governance requirements.

11.4.2 Integration with Existing Processes

Risk Management Integration (Month 14-17):

The AI governance framework must be fully integrated with existing risk management processes to ensure comprehensive and consistent risk oversight.

Risk Reporting Integration: AI risks should be integrated into existing risk reporting processes and structures. Integration requirements include:

- **Risk Register Integration:** Inclusion of AI risks in the institution's master risk register.
- **Risk Committee Reporting:** Regular reporting of AI risks to existing risk committees and governance bodies.
- **Risk Appetite Integration:** Integration of AI risk appetite with overall institutional risk appetite.
- **Capital Allocation:** Consideration of AI risks in capital allocation and stress testing processes.
- **Regulatory Reporting:** Integration of AI risk information into regulatory risk reports.

Control Framework Integration: AI governance controls should be integrated with existing control frameworks. This includes:

- **Internal Control Framework:** Integration of AI controls with existing internal control frameworks.
- **Operational Risk Framework:** Inclusion of AI operational risks in existing operational risk management processes.
- **Compliance Framework:** Integration of AI compliance requirements with existing compliance monitoring processes.
- **Audit Framework:** Integration of AI governance into internal audit planning and execution.
- **Business Continuity:** Integration of AI systems into business continuity and disaster recovery planning.

11.5 Phase 4: Optimization and Continuous Improvement (Months 19-24)

11.5.1 Process Optimization

Performance Analysis (Month 19-21):

Comprehensive analysis of governance framework performance provides the foundation for optimization and continuous improvement.

Effectiveness Assessment: Regular assessment of governance framework effectiveness should be conducted to identify areas for improvement. Assessment areas include:

- **Risk Management Effectiveness:** Evaluation of the effectiveness of AI risk management processes in identifying and mitigating risks.
- **Compliance Performance:** Assessment of compliance with regulatory requirements and internal policies.
- **Operational Efficiency:** Analysis of the efficiency of governance processes and their impact on AI development and deployment.
- **Stakeholder Satisfaction:** Evaluation of stakeholder satisfaction with governance processes and outcomes.
- **Cost-Benefit Analysis:** Analysis of the costs and benefits of the governance framework.

Benchmarking: Comparison with industry best practices and peer institutions provides insights for improvement [43]. Benchmarking activities should include:

- **Industry Standards:** Comparison with relevant industry standards and frameworks.
- **Peer Comparison:** Benchmarking against peer institutions where possible.
- **Best Practice Research:** Research into emerging best practices in AI governance.
- **Regulatory Guidance:** Monitoring of regulatory guidance and expectations for AI governance.

- **Technology Trends:** Assessment of emerging technologies and their implications for AI governance.

11.5.2 Continuous Improvement Framework

Improvement Process (Month 22-24):

A formal continuous improvement process should be established to ensure ongoing enhancement of the AI governance framework.

Feedback Mechanisms: Systematic feedback mechanisms should be implemented to capture input from all stakeholders [44]. These mechanisms should include:

- **Regular Surveys:** Periodic surveys of stakeholders to gather feedback on governance processes.
- **Focus Groups:** Regular focus groups with different stakeholder groups to gather detailed feedback.
- **Suggestion Systems:** Formal systems for submitting suggestions for governance improvements.
- **Incident Analysis:** Analysis of incidents and issues to identify improvement opportunities.
- **Performance Reviews:** Regular performance reviews of governance processes and outcomes.

Improvement Implementation: A structured process should be established for evaluating and implementing improvements. This process should include:

- **Improvement Evaluation:** Systematic evaluation of proposed improvements including cost-benefit analysis.
- **Prioritization:** Prioritization of improvements based on impact, feasibility, and resource requirements.
- **Implementation Planning:** Detailed planning for implementing approved improvements.
- **Change Management:** Comprehensive change management for governance process improvements.
- **Effectiveness Monitoring:** Monitoring of improvement effectiveness and impact on governance outcomes.

Future Roadmap Development: A forward-looking roadmap should be developed to guide future AI governance evolution [45]. The roadmap should address:

- **Emerging Technologies:** Consideration of emerging AI technologies and their governance implications.
- **Regulatory Evolution:** Anticipation of regulatory changes and their impact on governance requirements.
- **Business Strategy:** Alignment of AI governance evolution with business strategy and objectives.

- **Technology Trends:** Consideration of technological trends and their implications for governance infrastructure.
- **Capability Development:** Planning for future capability development needs in AI governance.

12. Compliance and Monitoring

12.1 Regulatory Compliance Framework

12.1.1 Compliance Program Structure

A comprehensive compliance program for AI systems must address both traditional banking regulations and AI-specific requirements.

Program Components:

1. **Compliance Policies:** Comprehensive policies addressing AI-specific compliance requirements
2. **Compliance Procedures:** Detailed procedures for ensuring ongoing compliance with AI regulations
3. **Compliance Monitoring:** Systematic monitoring of AI system compliance with regulatory requirements
4. **Compliance Testing:** Regular testing of AI compliance controls and procedures
5. **Compliance Reporting:** Regular reporting on AI compliance status and issues
6. **Compliance Training:** Comprehensive training programs on AI compliance requirements

Organizational Structure:

- Chief Compliance Officer: Overall responsibility for AI compliance program
- AI Compliance Manager: Specialized role for managing AI-specific compliance requirements
- Business Line Compliance: Compliance responsibilities within business lines using AI systems
- Compliance Testing: Independent testing of AI compliance controls and procedures
- Compliance Reporting: Regular reporting to senior management and board of directors
- Regulatory Relations: Management of relationships with regulators on AI compliance matters

Program Governance:

- Establish clear governance structure for AI compliance program

- Define roles and responsibilities for AI compliance activities
- Implement regular review and update of AI compliance program
- Conduct regular assessment of AI compliance program effectiveness
- Maintain documentation of AI compliance program activities and results
- Report AI compliance program status to senior management and regulators

12.1.2 Regulatory Mapping

Financial institutions must maintain comprehensive mapping of regulatory requirements applicable to AI systems [46].

Regulatory Inventory:

- **BDL Circulars:** Comprehensive inventory of applicable BDL circulars and their AI implications
- **Lebanese Laws:** Inventory of Lebanese laws applicable to AI systems in financial services
- **International Standards:** Relevant international standards and frameworks for AI governance
- **Industry Guidelines:** Industry best practices and guidelines for AI in financial services
- **Regulatory Updates:** Ongoing monitoring of regulatory developments and updates
- **Interpretation Guidance:** Documented interpretations of regulatory requirements for AI systems

Mapping Process:

- Conduct comprehensive analysis of regulatory requirements applicable to each AI system
- Document specific regulatory requirements and their implementation in AI systems
- Identify areas where guidance is not explicit and areas requiring interpretation or guidance
- Maintain mapping documentation and update regularly
- Conduct regular review of regulatory mapping with legal and compliance teams
- Report regulatory mapping results to senior management and AI governance committee

Compliance Assessment:

- Assess AI system compliance with mapped regulatory requirements
- Identify compliance gaps and develop remediation plans
- Monitor ongoing compliance with regulatory requirements
- Conduct regular compliance assessments and updates
- Document compliance assessment results and remediation efforts
- Report compliance assessment results to appropriate stakeholders

12.1.3 Compliance Testing

Regular testing of AI compliance controls is essential to ensure ongoing effectiveness [47].

Testing Program:

- **Risk-Based Testing:** Focus testing efforts on highest-risk AI systems and controls
- **Comprehensive Coverage:** Ensure testing covers all critical AI compliance controls
- **Independent Testing:** Use independent testers who are not involved in AI system operation
- **Regular Schedule:** Conduct testing on a regular schedule based on risk assessment
- **Issue Identification:** Identify compliance control deficiencies and weaknesses
- **Remediation Tracking:** Track remediation of identified compliance issues

Testing Methodologies:

- **Control Testing:** Test effectiveness of specific AI compliance controls
- **Process Testing:** Test end-to-end AI compliance processes and procedures
- **System Testing:** Test AI system compliance with regulatory requirements
- **Documentation Testing:** Test adequacy and accuracy of AI compliance documentation
- **Training Testing:** Test effectiveness of AI compliance training programs
- **Incident Testing:** Test AI compliance incident response procedures

Testing Documentation:

- Maintain comprehensive documentation of all AI compliance testing activities
- Document testing methodologies, procedures, and results
- Track remediation of identified compliance issues and deficiencies
- Report testing results to senior management and AI governance committee
- Maintain testing records for regulatory examination and audit purposes
- Update testing procedures based on lessons learned and regulatory changes

12.2 Performance Monitoring

12.2.1 Key Performance Indicators

Effective monitoring of AI systems requires comprehensive KPIs that address performance, risk, and compliance.

Performance KPIs:

- **Model Accuracy:** Accuracy metrics for AI model predictions and decisions
- **System Availability:** Uptime and availability metrics for AI systems
- **Response Time:** Response time metrics for AI system queries and transactions
- **Throughput:** Transaction processing capacity and throughput metrics

- **Error Rates:** Error rates and failure metrics for AI systems
- **User Satisfaction:** User satisfaction metrics for AI system interfaces and outputs

Risk KPIs:

- **Model Drift:** Metrics measuring changes in model performance over time
- **Data Quality:** Metrics measuring quality of data used in AI systems
- **Bias Metrics:** Metrics measuring fairness and bias in AI system outputs
- **Security Incidents:** Number and severity of security incidents affecting AI systems
- **Operational Incidents:** Number and impact of operational incidents in AI systems
- **Compliance Violations:** Number and severity of compliance violations in AI systems

Business KPIs:

- **Cost Efficiency:** Cost metrics for AI system operation and maintenance
- **Business Value:** Metrics measuring business value generated by AI systems
- **Customer Impact:** Metrics measuring impact of AI systems on customer experience
- **Process Efficiency:** Metrics measuring efficiency improvements from AI systems
- **Revenue Impact:** Metrics measuring revenue impact of AI systems
- **Risk Reduction:** Metrics measuring risk reduction achieved through AI systems

12.2.2 Monitoring Infrastructure

Robust monitoring infrastructure is essential for effective AI system oversight.

Monitoring Architecture:

- **Real-time Monitoring:** Real-time monitoring of AI system performance and behavior
- **Batch Monitoring:** Batch processing for comprehensive analysis of AI system data
- **Centralized Dashboard:** Centralized dashboard for monitoring all AI systems
- **Alerting System:** Automated alerting for AI system issues and anomalies
- **Data Storage:** Comprehensive data storage for AI system monitoring data
- **Reporting Tools:** Tools for generating AI system monitoring reports

Technical Components:

- **Data Collection:** Automated collection of AI system performance and operational data
- **Data Processing:** Processing and analysis of collected monitoring data
- **Anomaly Detection:** Automated detection of anomalies in AI system behavior
- **Trend Analysis:** Analysis of trends in AI system performance and behavior
- **Predictive Analytics:** Predictive analytics for anticipating AI system issues
- **Integration:** Integration with existing monitoring and management systems

Monitoring Procedures:

- Establish clear procedures for AI system monitoring and alerting
- Define escalation procedures for AI system issues and anomalies
- Implement regular review of monitoring data and trends
- Conduct periodic assessment of monitoring infrastructure effectiveness
- Maintain documentation of monitoring procedures and configurations
- Train staff on monitoring tools and procedures

12.2.3 Reporting and Analytics

Comprehensive reporting and analytics provide insights into AI system performance and effectiveness.

Reporting Framework:

- **Executive Reporting:** High-level reporting for senior management and board of directors
- **Operational Reporting:** Detailed operational reporting for AI system managers
- **Regulatory Reporting:** Specialized reporting for regulatory requirements
- **Risk Reporting:** Risk-focused reporting for risk management functions
- **Compliance Reporting:** Compliance-focused reporting for compliance functions
- **Performance Reporting:** Performance-focused reporting for business stakeholders

Analytics Capabilities:

- **Descriptive Analytics:** Analysis of historical AI system performance and behavior
- **Diagnostic Analytics:** Analysis to understand causes of AI system issues and trends
- **Predictive Analytics:** Predictive analysis of future AI system performance and risks
- **Prescriptive Analytics:** Recommendations for optimizing AI system performance
- **Comparative Analytics:** Comparison of AI system performance across different periods and systems
- **Benchmarking:** Benchmarking of AI system performance against industry standards

Reporting Automation:

- Implement automated generation of standard AI system reports
- Use self-service analytics tools for ad-hoc analysis and reporting
- Establish regular reporting schedules for different stakeholder groups
- Implement automated distribution of reports to appropriate stakeholders
- Provide interactive dashboards for real-time monitoring and analysis
- Maintain audit trails for all reporting and analytics activities

12.3 Audit and Assurance

12.3.1 Internal Audit Program

Internal audit plays a critical role in providing independent assurance on AI governance effectiveness.

Audit Program Structure:

- **AI Audit Strategy:** Comprehensive strategy for auditing AI systems and governance
- **Risk-Based Planning:** Risk-based approach to AI audit planning and execution
- **Audit Universe:** Comprehensive inventory of auditable AI systems and processes
- **Audit Schedule:** Regular schedule for AI audits based on risk assessment
- **Audit Resources**: Adequate resources and expertise for conducting AI audits
- **Audit Reporting:** Regular reporting of AI audit results to senior management and board

Audit Scope:

- **Governance Effectiveness**: Assessment of AI governance structure and processes
- **Risk Management:** Evaluation of AI risk management framework and controls
- **Compliance:** Assessment of compliance with AI-related regulatory requirements
- **Operational Controls:** Review of operational controls for AI systems
- **Data Governance:** Evaluation of data governance controls for AI systems
- **Third-Party Management:** Assessment of controls for third-party AI services

Audit Methodologies:

- Develop specialized audit methodologies for AI systems and processes
- Use data analytics and continuous auditing techniques for AI audit
- Implement risk-based sampling and testing approaches for AI audits
- Conduct both automated and manual testing of AI controls
- Use external experts and specialists for complex AI audit areas
- Document audit methodologies and update based on experience

12.3.2 External Assurance

External assurance provides additional validation of AI governance and controls.

External Audit:

- **Financial Statement Audit:** Consideration of AI systems in financial statement audits
- **IT Audit:** Specialized IT audit of AI systems and infrastructure
- **Compliance Audit:** External audit of AI compliance with regulatory requirements
- **Security Audit:** External security assessment of AI systems and controls

- **Model Validation:** Independent validation of AI models by external experts
- **Governance Review:** External review of AI governance framework and effectiveness

Regulatory Examination:

- **Examination Preparation:** Preparation for regulatory examinations of AI systems
- **Documentation Support:** Comprehensive documentation to support regulatory examinations
- **Issue Response:** Response to regulatory examination findings and recommendations
- **Remediation Planning:** Development of remediation plans for regulatory issues
- **Follow-up Activities**: Follow-up activities to address regulatory concerns
- **Ongoing Dialogue:** Ongoing dialogue with regulators on AI governance matters

Third-Party Assessments:

- **Certification Programs:** Participation in relevant AI certification programs
- **Industry Benchmarking:** Benchmarking of AI governance against industry peers
- **Best Practice Reviews:** Review of AI governance against industry best practices
- **Gap Assessments:** Independent assessment of AI governance gaps and opportunities
- **Maturity Assessments:** Assessment of AI governance maturity and development needs
- **Continuous Improvement:** Use of external assessments to drive continuous improvement

13. Future Considerations

13.1 Emerging Technologies

13.1.1 Generative AI

Generative AI technologies present new opportunities and risks that require specialized governance approaches.

Technology Characteristics:

- **Large Language Models:** AI systems capable of generating human-like text and responses
- **Multimodal Systems:** AI systems that can process and generate multiple types of content
- **Foundation Models:** Large-scale AI models that can be adapted for multiple use cases
- **Prompt Engineering:** Techniques for optimizing interactions with generative AI systems

- **Fine-tuning:** Customization of generative AI models for specific use cases
- **Retrieval-Augmented Generation:** Combining generative AI with information retrieval

Financial Services Applications:

- **Customer Service:** AI-powered chatbots and virtual assistants for customer support
- **Content Generation:** Automated generation of reports, summaries, and documentation
- **Code Generation:** AI-assisted software development and code generation
- **Research and Analysis:** AI-powered research and analysis of market and economic data
- **Regulatory Reporting:** AI-assisted preparation of regulatory reports and filings
- **Training and Education:** AI-powered training materials and educational content

Governance Considerations:

- Implement specialized governance frameworks for generative AI systems
- Address unique risks such as hallucination, bias amplification, and misinformation
- Establish human oversight requirements for generative AI outputs
- Implement content filtering and safety controls for generative AI systems
- Develop testing and validation procedures for generative AI applications
- Address intellectual property and copyright considerations for generated content

13.1.2 Quantum Computing

Quantum computing may significantly impact AI capabilities and security requirements.

Technology Impact:

- **Enhanced AI Capabilities:** Quantum computing may enable more powerful AI algorithms
- **Cryptographic Implications:** Quantum computing may compromise current encryption methods
- **Optimization Applications:** Quantum algorithms may improve optimization in financial modeling
- **Risk Modeling:** Quantum computing may enable more sophisticated risk modeling
- **Portfolio Optimization:** Quantum algorithms may improve portfolio optimization techniques
- **Fraud Detection:** Quantum-enhanced AI may improve fraud detection capabilities

Preparedness Strategies:

- Monitor developments in quantum computing and their implications for AI
- Assess potential impact of quantum computing on existing AI systems and security
- Develop quantum-resistant security measures for AI systems

- Explore potential applications of quantum computing in financial services
- Participate in industry initiatives on quantum computing and AI
- Maintain awareness of regulatory developments related to quantum computing

13.1.3 Edge AI

Edge AI technologies enable AI processing at the edge of networks, closer to data sources.

Technology Benefits:

- **Reduced Latency:** Lower latency for AI processing and decision-making
- **Data Privacy:** Enhanced privacy by processing data locally
- **Bandwidth Efficiency:** Reduced bandwidth requirements for AI applications
- **Offline Capability:** AI functionality even when disconnected from central systems
- **Real-time Processing:** Real-time AI processing for time-sensitive applications
- **Cost Efficiency:** Reduced costs for data transmission and cloud processing

Implementation Considerations:

- Assess potential applications of edge AI in financial services
- Develop governance frameworks for distributed AI systems
- Address security challenges of edge AI deployments
- Implement management and monitoring capabilities for edge AI systems
- Consider regulatory implications of distributed AI processing
- Develop skills and capabilities for edge AI development and management

13.2 Regulatory Evolution

13.2.1 International Regulatory Trends

Global regulatory developments in AI will likely influence Lebanese regulatory approaches.

Key Regulatory Trends:

- **Risk-Based Regulation:** Increasing adoption of risk-based approaches to AI regulation
- **Sector-Specific Rules:** Development of sector-specific AI regulations for financial services
- **International Coordination:** Increased coordination among international regulators
- **Standards Adoption**: Growing adoption of international AI standards and frameworks
- **Enforcement Actions:** Increasing regulatory enforcement actions related to AI systems
- **Transparency Requirements:** Enhanced requirements for AI system transparency and explainability

Preparation Strategies:

- Monitor international regulatory developments and their potential impact
- Participate in international forums and working groups on AI regulation
- Align AI governance frameworks with emerging international standards
- Prepare for potential adoption of international regulatory approaches in Lebanon
- Engage with regulators on AI governance and regulatory development
- Maintain flexibility to adapt to changing regulatory requirements

13.2.2 Lebanese Regulatory Development

BDL and other Lebanese regulators are likely to develop more specific AI regulations.

Anticipated Developments:

- **AI-Specific Circulars:** BDL may issue circulars specifically addressing AI in financial services
- **Enhanced Guidance:** More detailed guidance on interpreting existing regulations for AI
- **Approval Processes:** Formalized approval processes for AI systems in financial services
- **Reporting Requirements:** Enhanced reporting requirements for AI systems and incidents
- **Supervisory Expectations:** Clearer supervisory expectations for AI governance and risk management
- **Enforcement Actions:** Potential enforcement actions related to AI governance failures

Preparedness Actions:

- Engage proactively with BDL on AI governance and regulatory development
- Participate in industry consultations on AI regulation
- Maintain robust AI governance frameworks that can adapt to new requirements
- Document AI governance practices and decisions for regulatory review
- Prepare for enhanced regulatory scrutiny of AI systems
- Build relationships with regulators and industry peers on AI governance

13.3 Industry Evolution

13.3.1 AI Maturity Development

The financial services industry's AI maturity will continue to evolve, requiring adaptive governance approaches.

Maturity Stages:

- **Experimental:** Early experimentation with AI technologies and use cases

- **Pilot Implementation:** Pilot implementations of AI systems in limited use cases
- **Scaled Deployment:** Scaled deployment of AI systems across multiple use cases
- **Strategic Integration:** Strategic integration of AI into core business processes
- **AI-Native Operations:** AI-native operations with AI embedded throughout the organization
- **Ecosystem Integration:** Integration of AI across industry ecosystems and partnerships

Governance Evolution:

- Adapt governance frameworks to support increasing AI maturity
- Develop more sophisticated risk management approaches for complex AI systems
- Implement advanced monitoring and analytics capabilities for AI governance
- Build organizational capabilities for AI governance and management
- Establish industry partnerships and collaborations on AI governance
- Prepare for AI-native business models and operations

13.3.2 Ecosystem Development

The AI ecosystem in Lebanese financial services will continue to develop and mature.

Ecosystem Components:

- **Technology Providers:** Growing ecosystem of AI technology providers and vendors
- **Service Providers:** Specialized service providers for AI development and management
- **Regulatory Bodies:** Enhanced regulatory capabilities and expertise in AI oversight
- **Industry Associations:** Industry associations focused on AI governance and best practices
- **Academic Institutions:** Academic institutions providing AI research and education
- **International Partners:** International partnerships and collaborations on AI development

Participation Strategies:

- Actively participate in AI ecosystem development and industry initiatives
- Build partnerships with AI technology and service providers
- Collaborate with academic institutions on AI research and development
- Participate in industry associations and working groups on AI governance
- Engage with international partners on AI best practices and standards
- Contribute to the development of AI capabilities and expertise in Lebanon

13.4 Strategic Planning

13.4.1 Long-term AI Strategy

Financial institutions should develop long-term AI strategies that align with business objectives and regulatory requirements.

Strategy Components:

- **Vision and Objectives:** Clear vision and objectives for AI adoption and use
- **Use Case Roadmap:** Roadmap for AI use case development and implementation
- **Technology Strategy:** Strategy for AI technology selection and development
- **Capability Building:** Strategy for building AI capabilities and expertise
- **Partnership Strategy:** Strategy for AI partnerships and collaborations
- **Risk Management:** Long-term approach to AI risk management and governance

Strategic Considerations:

- Align AI strategy with overall business strategy and objectives
- Consider regulatory environment and potential changes in AI regulation
- Assess competitive landscape and industry trends in AI adoption
- Evaluate organizational readiness and capability requirements for AI
- Consider ethical and societal implications of AI strategy
- Plan for long-term sustainability and evolution of AI capabilities

13.4.2 Continuous Improvement

AI governance frameworks must incorporate continuous improvement mechanisms.

Improvement Areas:

- **Governance Effectiveness:** Regular assessment and improvement of governance effectiveness
- **Risk Management:** Continuous enhancement of AI risk management capabilities
- **Technology Capabilities:** Ongoing development of AI technology capabilities
- **Organizational Capabilities:** Continuous building of AI skills and expertise
- **Process Optimization:** Regular optimization of AI-related processes and procedures
- **Stakeholder Engagement:** Ongoing engagement with stakeholders on AI governance

Improvement Mechanisms:

- Implement regular review and assessment of AI governance framework
- Establish feedback mechanisms from stakeholders and users
- Monitor industry best practices and emerging trends in AI governance
- Conduct regular benchmarking against industry peers and standards

- Implement lessons learned processes for AI projects and initiatives
- Maintain flexibility to adapt to changing requirements and circumstances

14. Glossary of Terms

Artificial Intelligence (AI): Computer systems that can perform tasks that typically require human intelligence, including learning, reasoning, problem-solving, and decision-making.

Algorithm: A set of rules or instructions that a computer follows to solve problems or complete tasks.

Algorithmic Bias: Systematic and unfair discrimination in AI system outputs that disadvantages certain groups or individuals.

Artificial General Intelligence (AGI): AI systems that possess human-level cognitive abilities across a wide range of domains.

Artificial Neural Network: A computing system inspired by biological neural networks, consisting of interconnected nodes that process information.

Automated Decision-Making: The process of making decisions through technological means without human involvement.

Bias: Systematic errors or prejudices in AI systems that can lead to unfair or discriminatory outcomes.

Big Data: Extremely large datasets that require specialized tools and techniques to analyze effectively.

Business Continuity: The capability of an organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident.

Chatbot: An AI-powered software application designed to simulate conversation with human users.

Cloud Computing: The delivery of computing services over the internet, including servers, storage, databases, and software.

Compliance: Adherence to laws, regulations, guidelines, and specifications relevant to business operations.

Computer Vision: AI technology that enables computers to interpret and understand visual information from images or videos.

Data Governance: The overall management of data availability, usability, integrity, and security in an organization.

Data Mining: The process of discovering patterns and knowledge from large amounts of data.

Data Privacy: The protection of personal information from unauthorized access, use, or disclosure.

Data Quality: The degree to which data meets requirements for accuracy, completeness, consistency, and reliability.

Deep Learning: A subset of machine learning that uses artificial neural networks with multiple layers to model and understand complex patterns.

Differential Privacy: A mathematical framework for measuring and limiting privacy loss when analyzing datasets.

Digital Transformation: The integration of digital technology into all areas of business, fundamentally changing operations and value delivery.

Explainable AI (XAI): AI systems designed to provide clear explanations of their decision-making processes and outputs.

Feature Engineering: The process of selecting, modifying, or creating input variables for machine learning models.

Federated Learning: A machine learning approach where models are trained across decentralized data sources without centralizing the data.

Generative AI: AI systems capable of creating new content, including text, images, audio, or code.

Governance: The system of rules, practices, and processes by which an organization is directed and controlled.

Human-in-the-Loop: AI systems that incorporate human judgment and oversight in their decision-making processes.

Hyperparameter: Configuration settings used to control the learning process of machine learning algorithms.

Large Language Model (LLM): AI models trained on vast amounts of text data to understand and generate human-like language.

Machine Learning: A subset of AI that enables computers to learn and improve from experience without being explicitly programmed.

Model Drift: The degradation of a machine learning model's performance over time due to changes in data patterns.

Model Validation: The process of testing and verifying that a machine learning model performs as expected and meets requirements.

Natural Language Processing (NLP): AI technology that enables computers to understand, interpret, and generate human language.

Operational Risk: The risk of loss resulting from inadequate or failed internal processes, people, systems, or external events.

Overfitting: A modeling error where a machine learning model performs well on training data but poorly on new, unseen data.

Predictive Analytics: The use of data, statistical algorithms, and machine learning techniques to identify future outcomes.

Privacy by Design: An approach that embeds privacy considerations into the design and operation of systems from the outset.

Reinforcement Learning: A machine learning approach where agents learn to make decisions by receiving rewards or penalties for their actions.

Risk Management: The identification, assessment, and prioritization of risks followed by coordinated efforts to minimize their impact.

Robotic Process Automation (RPA): Technology that uses software robots to automate repetitive, rule-based tasks.

Supervised Learning: A machine learning approach that uses labeled training data to learn the relationship between inputs and outputs.

Three Lines of Defense: A risk management framework that defines three levels of risk management and control within an organization.

Training Data: The dataset used to teach machine learning algorithms to make predictions or decisions.

Transfer Learning: A machine learning technique where a model developed for one task is adapted for a related task.

Transparency: The degree to which AI systems and their decision-making processes can be understood and explained.

Unsupervised Learning: A machine learning approach that finds patterns in data without using labeled examples.

Validation Set: A dataset used to evaluate machine learning model performance during development and tuning.

Version Control: The management of changes to documents, programs, and other collections of information over time.

15. Appendices

Appendix A: AI Compliance Checklist

This comprehensive checklist provides a structured approach to ensuring compliance with AI governance requirements. The checklist is organized by governance area and includes specific requirements, implementation guidance, and verification criteria.

Governance Area	Requirement	Implementation Status	Evidence/Documentation	Responsible Party	Target Date	Verification Method
Governance Structure						
AI Governance Committee established	Committee charter approved and members appointed	☐ Complete ☐ In Progress ☐ Not Started	Committee charter, member appointments	Chief Risk Officer	Month 2	Document review
AI Risk Management Office operational	Office established with appropriate staffing	☐ Complete ☐ In Progress ☐ Not Started	Organizational chart, job descriptions	Chief Risk Officer	Month 3	Organizational review
Roles and responsibilities defined	Clear RACI matrix for AI governance	☐ Complete ☐ In Progress ☐ Not Started	RACI matrix, role descriptions	AI Governance Committee	Month 3	Document review
Policy Framework						
Master AI Governance Policy approved	Policy approved by AI Governance Committee	☐ Complete ☐ In Progress ☐ Not Started	Approved policy document	AI Governance Committee	Month 6	Policy review
AI Risk Management Policy implemented	Detailed risk management procedures in place	☐ Complete ☐ In Progress ☐ Not Started	Risk management procedures	AI Risk Manager	Month 9	Process review

Governance Area	Requirement	Implementation Status	Evidence/Documentation	Responsible Party	Target Date	Verification Method
AI Ethics Policy established	Ethical guidelines for AI development and deployment	☐ Complete ☐ In Progress ☐ Not Started	Ethics policy document	AI Governance Committee	Month 9	Policy review
Risk Management						
AI risk assessment framework implemented	Standardized risk assessment methodology	☐ Complete ☐ In Progress ☐ Not Started	Risk assessment templates	AI Risk Manager	Month 9	Framework review
Risk monitoring systems operational	Continuous monitoring of AI system risks	☐ Complete ☐ In Progress ☐ Not Started	Monitoring dashboards	AI Risk Manager	Month 12	System demonstration
Risk reporting processes established	Regular risk reporting to governance bodies	☐ Complete ☐ In Progress ☐ Not Started	Risk reports, meeting minutes	AI Risk Manager	Month 12	Report review
Model Management						
Model validation framework implemented	Comprehensive model validation procedures	☐ Complete ☐ In Progress ☐ Not Started	Validation procedures, test results	Model Risk Specialist	Month 12	Validation review
Model monitoring systems operational	Continuous monitoring of model performance	☐ Complete ☐ In Progress ☐ Not Started	Monitoring systems, alerts	Model Risk Specialist	Month 15	System review
Model documentation standards implemented	Standardized documentation for all AI models	☐ Complete ☐ In Progress ☐ Not Started	Model documentation templates	AI Development Teams	Month 15	Documentation review
Data Governance						

Governance Area	Requirement	Implementation Status	Evidence/Documentation	Responsible Party	Target Date	Verification Method
Data quality standards implemented	Clear standards for AI training and operational data	☐ Complete ☐ In Progress ☐ Not Started	Data quality procedures	Chief Data Officer	Month 12	Process review
Data lineage tracking operational	Comprehensive tracking of data sources and transformations	☐ Complete ☐ In Progress ☐ Not Started	Data lineage documentation	Chief Data Officer	Month 15	System review
Privacy protection measures implemented	Appropriate privacy controls for AI data processing	☐ Complete ☐ In Progress ☐ Not Started	Privacy impact assessments	Chief Data Officer	Month 12	Assessment review
Regulatory Compliance						
BDL notification/approval processes established	Clear processes for notifying/engaging BDL of AI systems	☐ Complete ☐ In Progress ☐ Not Started	Notification/approval procedures	Chief Compliance Officer	Month 6	Process review
Regulatory reporting capabilities implemented	Systems for generating required regulatory reports	☐ Complete ☐ In Progress ☐ Not Started	Reporting systems	Chief Compliance Officer	Month 15	System review
Compliance monitoring systems operational	Continuous monitoring of regulatory compliance	☐ Complete ☐ In Progress ☐ Not Started	Compliance dashboards	Chief Compliance Officer	Month 15	System demonstration
Third-Party Management						
Vendor assessment framework implemented	Standardized assessment of AI vendors	☐ Complete ☐ In Progress ☐ Not Started	Vendor assessment procedures	Procurement/Risk	Month 12	Framework review
Contract standards established	Standard contract terms for AI vendors	☐ Complete ☐ In Progress	Contract templates	Legal/Procurement	Month 9	Template review

Governance Area	Requirement	Implementation Status	Evidence/Documentation	Responsible Party	Target Date	Verification Method
		☐ Not Started				
Vendor monitoring processes operational	Ongoing monitoring of AI vendor performance	☐ Complete ☐ In Progress ☐ Not Started	Monitoring procedures	Vendor Management	Month 15	Process review
Training and Awareness						
AI governance training program implemented	Comprehensive training for all relevant staff	☐ Complete ☐ In Progress ☐ Not Started	Training materials, completion records	Human Resources	Month 18	Training review
Awareness campaigns conducted	Regular awareness campaigns on AI governance	☐ Complete ☐ In Progress ☐ Not Started	Campaign materials, metrics	Communications	Ongoing	Campaign review
Competency assessments completed	Assessment of staff competency in AI governance	☐ Complete ☐ In Progress ☐ Not Started	Assessment results	Human Resources	Month 18	Assessment review

Appendix B: AI Risk Assessment Template

This template provides a structured approach to conducting comprehensive risk assessments for AI systems. The template should be completed for each AI system and updated regularly to reflect changes in risk profile.

B.1 System Information

System Name: _____

System Owner: _____

Business Line: _____

Assessment Date: _____

Assessor: _____

Review Date: _____

B.2 System Description

Business Purpose: Provide a clear description of the business purpose and objectives of the AI system.

Use Cases: List the specific use cases and applications of the AI system.

Target Users: Identify the intended users of the AI system, both internal and external.

Integration Points: Describe how the AI system integrates with other systems and processes.

B.3 Technical Architecture

Model Type:

☐ Supervised Learning

☐ Unsupervised Learning

☐ Reinforcement Learning

☐ Deep Learning

☐ Other: _____

Algorithm Details: Provide details of the algorithms and techniques used in the AI system.

Data Sources: List all data sources used for training and operation of the AI system.

Infrastructure: Describe the technical infrastructure supporting the AI system.

B.4 Risk Assessment

Model Risk Assessment:

Risk Factor	Risk Level	Likelihood	Impact	Mitigation Measures	Residual Risk
Model Accuracy	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Model Bias	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Model Drift	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Explainability	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High

Operational Risk Assessment:

Risk Factor	Risk Level	Likelihood	Impact	Mitigation Measures	Residual Risk
System Availability	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Data Quality	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Security Vulnerabilities	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High

Risk Factor	Risk Level	Likelihood	Impact	Mitigation Measures	Residual Risk
Human Error	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High

Compliance Risk Assessment:

Risk Factor	Risk Level	Likelihood	Impact	Mitigation Measures	Residual Risk
Regulatory Approval	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Data Protection	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Consumer Protection	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High
Financial Regulations	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High	☐ Low ☐ Medium ☐ High		☐ Low ☐ Medium ☐ High

B.5 Overall Risk Assessment

Overall Risk Rating: ☐ Low ☐ Medium ☐ High ☐ Critical

Risk Justification: Provide justification for the overall risk rating based on individual risk assessments.

Key Risk Factors: Identify the most significant risk factors that contribute to the overall risk rating.

Recommended Actions: List specific actions recommended to address identified risks.

B.6 Approval and Sign-off

Risk Assessment Completed By:

Name: _____ Date: _____

Signature: _____

Reviewed and Approved By:

Name: _____ Date: _____

Title: _____

Signature: _____

B.7 AI Model Inventory

System Owner	Criticality Tier	Data Classifications Processed	Training Data Location	Model Type	Third-party Involvement	BDL Approval Status

Appendix C: Model Documentation Template

This template provides a standardized format for documenting AI models throughout their lifecycle. Complete documentation is essential for model governance, validation, and regulatory compliance.

C.1 Model Overview

Model Name: _____

Model Version: _____

Development Team: _____

Model Owner: _____

Documentation Date: _____

Last Updated: _____

C.2 Business Context

Business Objective: Clearly describe the business objective that the model is designed to achieve.

Use Case Description: Provide a detailed description of the specific use case and application of the model.

Success Criteria: Define the criteria that will be used to measure the success of the model.

Stakeholders: List of all stakeholders who are involved in or affected by the model.

C.3 Data Description

Training Data:

Data Source	Description	Size	Time Period	Quality Assessment

Feature Description:

Feature Name	Data Type	Description	Source	Transformation

Data Quality Checks: Describe the data quality checks performed on the training data.

Data Preprocessing: Detail all data preprocessing steps including cleaning, transformation, and feature engineering.

C.4 Model Architecture

Algorithm Type:

☐ Linear Regression

☐ Logistic Regression

☐ Decision Tree

☐ Random Forest

☐ Neural Network

☐ Other: _____

Model Architecture: Provide detailed description of the model architecture including layers, parameters, and configuration.

Hyperparameters:

Parameter	Value	Justification

Training Process: Describe the model training process including optimization algorithms, loss functions, and training procedures.

C.5 Model Performance

Performance Metrics:

Metric	Training Set	Validation Set	Test Set	Benchmark
Accuracy				
Precision				
Recall				
F1 Score				
AUC-ROC				

Model Validation: Describe the validation methodology used to assess model performance.

Cross-Validation Results: Provide results from cross-validation testing.

Robustness Testing: Describe robustness testing performed, and results obtained.

C.6 Model Limitations

Known Limitations: List known limitations of the model including performance limitations, data limitations, and use case limitations.

Assumptions: Document key assumptions made during model development.

Uncertainty Quantification: Describe how uncertainty in model predictions is quantified and communicated.

Edge Cases: Identify edge cases where the model may not perform as expected.

C.7 Ethical Considerations

Bias Assessment: Describe bias testing performed and results obtained.

Fairness Metrics:

Group	Demographic Parity	Equalized Odds	Calibration

Explainability: Describe the explainability features of the model and how explanations are generated.

Social Impact: Assess the potential social impact of the model deployment.

C.8 Deployment Information

Deployment Environment: Describe the production environment where the model is deployed.

Integration Details: Provide details of how the model integrates with existing systems and processes.

Monitoring Setup: Describe the monitoring systems in place for the deployed model.

Rollback Procedures: Document procedures for rolling back the model in case of issues.

C.9 Maintenance and Updates

Retraining Schedule: Define the schedule for model retraining and updates.

Performance Monitoring: Describe ongoing performance monitoring procedures.

Drift Detection: Detail drift detection mechanisms and response procedures.

Version Control: Describe version control procedures for model updates.

C.10 Approval and Sign-off

Model Documentation Completed By:

Name: _____ Date: _____

Role: _____

Signature: _____

Technical Review:

Name: _____ Date: _____

Role: _____

Signature: _____

Business Approval:

Name: _____ Date: _____

Role: _____

Signature: _____

Risk Management Approval:

Name: _____ Date: _____

Role: _____

Signature: _____

Appendix D: Related Resources

This appendix provides a comprehensive list of resources relevant to AI governance in Lebanese financial institutions, including regulatory documents, international standards, and best practice guides.

D.1 Lebanese Regulatory Documents

BDL Circulars:

- BDL Basic Circular 69/2000 - Electronic Banking Operations

- BDL Basic Circular 144/2017 - Cybersecurity and cybercrime prevention

- BDL Basic Circulars 123/2009 & 141/2017 – Business Continuity/Recovery Planning

- BDL Basic Circular 128/2013 - Compliance and outsourcing governance framework

- BDL Basic Circular 146/2018 - Data protection and customer information privacy requirements

Lebanese Laws:

- Banking Secrecy Law (1956) and Amendments

- Law 81/2018 - Electronic Transactions and Data Protection

D.2 International Standards and Frameworks

ISO Standards:

- ISO/IEC 42001:2023 - Artificial Intelligence Management Systems [Available at: https://www.iso.org/standard/81230.html]

- ISO/IEC 27001:2022 - Information Security Management Systems - ISO 31000:2018 - Risk Management Guidelines

NIST Frameworks:

- NIST AI Risk Management Framework (AI RMF 1.0) [Available at: https://www.nist.gov/itl/ai-risk-management-framework]

- NIST Cybersecurity Framework [Available at: https://www.nist.gov/cyberframework]

EU Regulations:

- EU AI Act (Regulation 2024/1689) [Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj]

- General Data Protection Regulation (GDPR) [Available at: https://gdpr-info.eu/]

D.3 Industry Best Practices

Financial Services:

- Basel Committee on Banking Supervision - Implications of fintech developments for banks and bank supervisors.

- Financial Stability Board - Artificial Intelligence and Machine Learning in Financial Services

- Institute of International Finance - Machine Learning in Credit Risk

AI Ethics, Evaluation, and Governance:

- Partnership on AI - Tenets [Available at: https://www.partnershiponai.org/tenets/]

- Montreal Declaration for Responsible AI

- IEEE 3128-2025: Recommended Practice for the Evaluation of Artificial Intelligence (AI) Dialogue System Capabilities

- IEEE 2841™-2022: Recommended Practice for Framework and Process for Deep Learning Evaluation

- IEEE 2842™-2021: Recommended Practice for Secure Multi-Party Computation

- IEEE 3119-2025: Standard for the Procurement of Artificial Intelligence and Automated Decision Systems

- IEEE P7015: Draft Standard for Data and Artificial Intelligence (AI) Literacy, Skills, and Readiness

- IEEE 2840-2024: Standard for Responsible AI Licensing

- IEEE P7100 EIAI: Working Group for Environmental Impacts of Artificial Intelligence

AI Development Best Practices:

- Google AI Principles [Available at: https://ai.google/principles/]

- Microsoft Responsible AI Principles [Available at: https://www.microsoft.com/en-us/ai/responsible-ai]

- IBM AI Ethics Board [Available at: https://www.ibm.com/artificial-intelligence/ethics]

D.5 Training and Certification

Professional Certifications:

- Certified AI Governance Professional (CAIGP)

- Certified Information Systems Auditor (CISA)

Training Resources:

- Coursera AI for Everyone Course

- edX MIT Introduction to Machine Learning

- Stanford CS229 Machine Learning Course

- MIT Professional Education AI Programs

D.6 Industry Organizations

Lebanese Organizations:

- Association of Banks in Lebanon (ABL)

International Organizations:

- ISACA (Information Systems Audit and Control Association)

16. References

[1] PwC UK. (2023). *AI in financial services: navigating the risk - opportunity equation*. Available at: https://www.pwc.co.uk/industries/financial-services/understanding-regulatory-developments/ai-in-financial-services-navigating-the-risk-opportunity-equation.html

[2] Naboulsi, A. A. R. (2025). Lebanese FinTech BDL Compliance Guide. Lebanese Financial Technology Association.

[3] European Parliament and Council. (2024). Regulation (EU) 2024/1689 on Artificial Intelligence (AI Act). Official Journal of the European Union. Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[4] National Institute of Standards and Technology. (2023). AI Risk Management Framework (AI RMF 1.0). U.S. Department of Commerce. Available at: https://www.nist.gov/itl/ai-risk-management-framework

[5] Lebanese Parliament. (1956). *Law of 3 September 1956 on Banking Secrecy (Law No. 133).* Official Gazette of the Republic of Lebanon.

[6] Banque du Liban. (2000, October 19). *Basic Circular No. 69 – Electronic Banking and Financial Operations.* Retrieved from https://www.bdl.gov.lb/basiccirculars.php

[7] Banque du Liban. (2017, November 28). *Basic Circular No. 144 – Prevention of Cybercrime (Decision No. 12725).* Retrieved from

https://www.bdl.gov.lb/CB%20Com/Laws%20And%20Regulations/Basic%20Circulars/Decision_12725_EN§1410_3.pdf

[8] Banque du Liban. *BDL Basic Circulars 123/2009 & 141/2017– Recovery and Business Continuity Plans.* Retrieved from https://www.bdl.gov.lb/basiccirculars.php

[9] Banque du Liban. (2013, January 12). *Basic Circular No. 128 – Compliance and Outsourcing Arrangements.* Retrieved from https://www.bdl.gov.lb/basiccirculars.php

[10] Banque du Liban. (2018, December 27). *Basic Circular No. 146 – Data Protection and Customer Information Privacy.* Retrieved from https://www.bdl.gov.lb/basiccirculars.php

[11] Lebanese Parliament. (1956). *Law of 3 September 1956 on Banking Secrecy (Law No. 133).* Official Gazette of the Republic of Lebanon.

[12] Republic of Lebanon. (2018). Law 81/2018 - Electronic Transactions and Data Protection. Lebanese Official Gazette. Available at: https://www.legallaw.ul.edu.lb/Law81-2018.pdf

[13] International Organization for Standardization. (2023). ISO/IEC 42001:2023 - Artificial Intelligence Management Systems. Available at: https://www.iso.org/standard/81230.html

[14] EuroMeSCo. (2024). Digital Sovereignty in the MENA Region: Overcoming Paradoxes to Ensure Digital Resilience. Available at: https://www.euromesco.net/publication/digital-sovereignty-in-the-mena-region-overcoming-paradoxes-to-ensure-digital-resilience

[15] The EU Artificial Intelligence Act. https://artificialintelligenceact.eu/article/14/#:~:text=The%20goal%20of%20human%20oversight,or%20implemented%20by%20the%20user.

[16] Montreal Declaration for Responsible AI. (2018). Ethical Principles for AI Development and Deployment. Available at: https://www.montrealdeclaration-responsibleai.com/

[17] Goodfellow, I., Shlens, J., & Szegedy, C. (2014). Explaining and Harnessing Adversarial Examples. International Conference on Learning Representations.

[18] Republic of Lebanon. Amendment to Banking Secrecy Law.

[19] Institute of Electrical and Electronics Engineers. (2023). IEEE Standards for Artificial Intelligence and Machine Learning. Available at: https://standards.ieee.org/initiatives/artificial-intelligence-systems/

[20] Financial Stability Board. (2017). Artificial Intelligence and Machine Learning in Financial Services - Regulatory and Supervisory Issues. Available at: https://www.fsb.org/uploads/P011117.pdf

[21] Basel Committee on Banking Supervision. (2017). Sound Practices: Implications of fintech developments for banks and bank supervisors. https://www.bis.org/bcbs/publ/d415.pdf

[22] Banco de España. (2023). Machine Learning in Credit Risk: Principles for Sound Implementation. MACHINE LEARNING IN CREDIT RISK: MEASURING THE DILEMMA BETWEEN PREDICTION AND SUPERVISORY COST. Available at: https://www.bde.es/f/webbde/SES/Secciones/Publicaciones/PublicacionesSeriadas/DocumentosTrabajo/20/Files/dt2032e.pdf

[23] Institute of Internal Auditors. (2024). Artificial Intelligence 101 Internal Auditors. Available at: https://www.theiia.org/en/content/tools/professional/2023/artificial-intelligence-101-for-internal-auditors

[24] Federal Reserve. (2011). Supervisory Guidance on Model Risk Management (SR 11-7). Board of Governors of the Federal Reserve System.

[25] Basel Committee on Banking Supervision. (2021). Principles for Operational Resilience. Bank for International Settlements. https://www.bis.org/bcbs/publ/d516.htm

[26] European Banking Authority. (2022). Guidelines on ICT and Security Risk Management. Available at: https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-ict-and-security-risk-management

[27] Barocas, S., Hardt, M., & Narayanan, A. (2023). Fairness and Machine Learning: Limitations and Opportunities. MIT Press.

[28] National Association of Corporate Directors. (2023). AI Governance for Boards: A Director's Guide. Available at: https://www.nacdonline.org/insights/publications.cfm?ItemNumber=74521

[29] McKinsey & Company. (2025). The State of AI Governance in Financial Services. McKinsey Global Institute. Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/quantumblack/our%20insights/the%20state%20of%20ai/2025/the-state-of-ai-how-organizations-are-rewiring-to-capture-value_final.pdf

[30] Deloitte. AI in Financial Services. Deloitte Center for Financial Services. Available at: https://www.deloitte.com/us/en/insights/research-centers/center-for-financial-services/ai-in-financial-services.html

[31] PwC. (2023). Artificial Intelligence for banks. Available at: https://www.pwc.com/cz/en/assets/AI-bank_21.08.2023_END.pdf

[32] KPMG. (2023). Responsible AI and the challenge of AI risk. Available at: https://kpmg.com/us/en/articles/2023/artificial-intelligence-survey-23.html

[33] Ernst & Young. (2024). How can cybersecurity transform to accelerate value from AI? Available at: https://www.ey.com/en_gl/insights/consulting/transform-cybersecurity-to-accelerate-value-from-ai

[34] Accenture. The age of AI: Banking's new reality. Available at: https://www.accenture.com/content/dam/accenture/final/accenture-com/document-2/Accenture-Age-AI-Banking-New-Reality.pdf

[35] Center for Democracy & technology. (2024). Best Practices in AI Documentation: The Imperative of Evidence from Practice. Available at: https://cdt.org/insights/best-practices-in-ai-documentation-the-imperative-of-evidence-from-practice/

[36] Boston Consulting Group. (2024). Digital & (Gen) AI Maturity: A Call to Action for Central Banks in a Rapidly Evolving Market. Available at: https://media-publications.bcg.com/BCG-2024-Digital-Gen-AI-Maturity-A-Call-to-Action-for-Central-Banks-in-a-Rapidly-Evolving-Market.pdf?linkId=719013555

[37] Capgemini. Setting the pace for intelligent transformation in banking with AI. Available at: https://www.capgemini.com/insights/research-library/setting-the-pace-for-intelligent-transformation/

[38] OECD. (2025). Governing with Artificial Intelligence. Available at: https://www.oecd.org/en/publications/governing-with-artificial-intelligence_795de142-en.html#:~:text=A%20key%20contributing%20factor%20being,All%20series%20are%20visible.

[39] Communicate Online. (2024). Adapting Responsible AI: Strategies for Businesses in the Middle East. Available at: https://communicateonline.me/news/adapting-responsible-ai-strategies-for-businesses-in-the-middle-east

[40] Creatio. (2025). AI Governance - Why Responsible AI Oversight Is Essential. Available at: https://www.creatio.com/glossary/ai-governance

[41] Mckinsey. (2024). Extracting value from AI in banking: Rewiring the enterprise. Available at: https://www.mckinsey.com/industries/financial-services/our-insights/extracting-value-from-ai-in-banking-rewiring-the-enterprise

[42] Palo Alto. Available at: https://www.paloaltonetworks.com/cyberpedia/ai-risk-management-framework

[43] ACA Group. (2024). Financial Services Firms Lag in AI Governance and Compliance Readiness, Survey Reveals. Available at: https://www.acaglobal.com/news-and-announcements/financial-services-firms-lag-ai-governance-and-compliance-readiness-survey-reveals

[44] FINOS AI Governance Framework. Human Feedback Loop for AI Systems. https://air-governance-framework.finos.org/mitigations/mi-11_human-feedback-loop-for-ai-systems.html

[45] Harvard Law School Forum on Corporate Governance. (2025). Strategic Governance of AI: A Roadmap for the Future. Available at: https://corpgov.law.harvard.edu/

[46] Financial Action Task Force. (2025). Financial Inclusion and Anti-Money Laundering and Terrorist Financing Measures. FATF Guidance. Available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Financial-Inclusion%20-Anti-Money-Laundering-Terrorist-Financing-Measures.pdf.coredownload.pdf

[47] European Securities and Markets Authority. (2023). AI in EU Securities Markets. Regulatory Considerations. ESMA Technical Standards. Available at: https://www.esma.europa.eu/sites/default/files/library/ESMA50-164-6247-AI_in_securities_markets.pdf

Summary Tables

Key Regulatory Requirements Summary

Regulation	Applicability to AI	Key Requirements	Implementation Priority
BDL Circular 69/2000	Customer-facing AI systems	BDL notification or approval, Technology Infrastructure Assessment	High
BDL Circular 144/2017	All AI systems	Cybersecurity measures, encryption, access controls	High
BDL Basic Circulars 123/2009 & 141/2017	Business-critical AI	Business continuity planning, disaster recovery	Medium
BDL Circular 128/2013	Third-party AI services	Due diligence, ongoing monitoring, accountability	Medium
Banking Secrecy Law and Amendments	AI processing customer data	Data confidentiality, access restrictions	High
Law 81/2018	AI processing personal data	Data subject rights, consent management	Medium

AI Risk Categories and Mitigation Strategies

Risk Category	Key Risks	Mitigation Strategies	Monitoring Frequency
Model Risk	Accuracy degradation, bias, drift	Model validation, performance monitoring, bias testing	Continuous
Operational Risk	System failures, data quality issues	Redundancy, quality controls, incident response	Real-time
Compliance Risk	Regulatory violations, approval issues	Compliance monitoring, regulatory engagement	Monthly

Ethical Risk	Bias, discrimination, transparency	Fairness testing, explainability, ethics review	Quarterly
Security Risk	Data breaches, adversarial attacks	Encryption, access controls, threat monitoring	Continuous

Implementation Phase Deliverables

Phase	Duration	Key Deliverables	Success Criteria
Phase 1: Foundation	Months 1-6	Governance committee, current state assessment, initial policies	Committee operational, gaps identified, policies approved
Phase 2: Framework Development	Months 7-12	Complete policies, pilot implementation, technology infrastructure	Policies implemented, pilots successful, systems operational
Phase 3: Full Implementation	Months 13-18	Framework rollout, process integration, staff training	All systems governed, processes integrated, staff trained
Phase 4: Optimization	Months 19-24	Process optimization, continuous improvement, future roadmap	Optimized processes, improvement framework, roadmap approved

---

Contact Information / Feedback

For questions or feedback regarding this guide, please contact the Governance & Compliance Department at Compliance@c-o.com.

Contact Author: https://www.linkedin.com/in/abed-al-rahman-naboulsi/