IJISEM
INTERNATIONAL JOURNAL OF INNOVATIONS IN SCIENCE ENGINEERING AND MANAGEMENT

OPEN ACCESS

Volume: 4

Issue: 3

Month: July

Year: 2025

ISSN: 2583-7117

Published: 11.07.2025

Citation:

Satyadhar Joshi "Gen AI in Financial Cybersecurity: A Comprehensive Review of Architectures, Algorithms, and Regulatory Challenges" International Journal of Innovations in Science Engineering and Management, vol. 4, no. 3, 2025, pp. 73–88.

DOI:

10.69968/ijisem.2025v4i373-88

Gen AI in Financial Cybersecurity: A Comprehensive Review of Architectures, Algorithms, and Regulatory Challenges

Satyadhar Joshi[1]

[1]*Independent Researcher Alumnus, International MBA, Bar-Ilan University, Israel Alumnus, Touro College MSIT, NY, USA.*

Abstract

This paper provides a comprehensive review of the intersection of cybersecurity, generative AI, and risk within the financial sector. We explore how AI is being leveraged for both defensive and offensive purposes, the emerging threats posed by GenAI, and the critical need for robust risk management frameworks and regulatory guidance. This paper reviews the intersection of cybersecurity, generative artificial intelligence (AI), and risk management in the financial sector. We examine the dual role of AI as both a tool for enhancing cybersecurity defenses and a vector for sophisticated cyber threats. The paper analyzes regulatory responses, emerging best practices, and the evolving threat landscape, with particular attention to generative AI's impact on financial institutions' risk profiles. We synthesize insights from recent industry reports, regulatory guidance, and academic literature to provide a comprehensive overview of current challenges and future directions in this critical domain. This paper presents a comprehensive review of AI-driven cybersecurity framework designed for financial institutions, integrating data analysis, risk assessment, and decision-making processes. The frameworks reviewed are structured around the DIKW (Data, Information, Knowledge, Wisdom) pyramid, which transforms raw data into actionable insights through natural language processing (NLP) and thematic extraction. Key components include a modular system architecture that processes data from multiple sources (e.g., transaction logs, threat feeds) using AI models, a risk engine for scoring threats, and a decision tree for implementing mitigation strategies. Anomaly detection is achieved through Isolation Forest and auto encoder models, with thresholds ($\tau = 0.6$ and $\tau = 0.5$, respectively) calibrated to balance sensitivity and specificity. The decision logic incorporates rules such as automatic blocking for high-risk transactions (scores ¿ 0.95) and multi-factor authentication (MFA) for non-whitelisted locations. Visualizations demonstrate the system's effectiveness in identifying and responding to threats while maintaining regulatory compliance.

Keywords; Cybersecurity, Generative AI, Artificial Intelligence, Financial Sector, Risk Management, Financial Institutions, AI Governance, Regulatory Compliance, Cyber Threats.

INTRODUCTION

The financial sector's digital transformation has accelerated with the adoption of artificial intelligence (AI), particularly generative AI technologies [1]. While these innovations offer unprecedented opportunities for efficiency, customer service, and risk management, they also introduce complex cybersecurity challenges [2]. Financial institutions now operate in an environment where AI serves both as a defensive tool against cyber threats and as an offensive weapon in the hands of malicious actors [3].

Recent regulatory guidance, such as the New York Department of Financial Services (NYDFS) October 2024 letter on AI-related cybersecurity risks, highlights the growing concern among policymakers [4], [5]. This paper examines three critical dimensions: (1) AI-enhanced cybersecurity threats facing financial institutions, (2) AI-driven risk management solutions, and (3) the evolving regulatory landscape for AI in finance.

The integration of artificial intelligence (AI), especially generative models, is reshaping the cybersecurity landscape in financial services.

While AI enhances automation and threat detection, it also introduces new vectors for sophisticated attacks such as deepfakes and adversarial manipulation [2], [6], [7]. This paper reviews the evolving risks, regulatory responses, and mitigation strategies relevant to financial institutions.

The financial sector, a cornerstone of global economies, is undergoing a significant transformation driven by digital innovation. At the forefront of this evolution is Artificial Intelligence (AI), with Generative AI (GenAI) emerging as a particularly disruptive force [1]. AI's integration promises enhanced efficiency, improved decision-making, and sophisticated risk management capabilities [8]–[12]. However, this technological embrace also ushers in a new era of cyber- security challenges and risks that financial institutions must meticulously address [2], [13]–[15]. This paper reviews the intricate relationship between cybersecurity, generative AI, and risk within the financial services industry.

TOP 10 KEY TERMS AND THEORETICAL CONCEPTS

This section identifies and explains the most critical terms, theories, and technical concepts at the intersection of cybersecurity, generative AI, and financial risk management.

1. Adversarial Machine Learning [19]

Techniques that exploit vulnerabilities in AI systems, including model evasion, data poisoning, and membership inference attacks, particularly dangerous for financial fraud detection systems.

2. AI Governance Frameworks [25]

Structured approaches for managing AI risks, encompassing model validation, ethical guidelines, and compliance mechanisms required by financial regulators.

3. Deepfake Financial Fraud [17]

The use of generative AI to create synthetic media (voices, videos) for impersonation attacks against financial institutions and their customers.

4. Explainable AI (XAI) [30]

Methods to make AI decision-making transparent, critical for meeting financial regulatory requirements and maintaining audit trails.

5. Generative Adversarial Networks (GANs) [31]

AI architectures that can generate synthetic financial data for testing fraud detection systems while also being weaponized by attackers.

6. Model Drift [32]

The phenomenon where AI models degrade over time as financial data distributions change, creating compliance and risk assessment challenges.

7. Quantum Risk Posture [27]

Emerging framework for assessing financial institution vulnerabilities to quantum computing attacks on cryptographic systems.

8. Responsible AI Principles [1]

Guidelines ensuring AI systems in finance are fair, accountable, and transparent, as promoted by OECD and financial regulators.

9. Third-Party AI Risk [21]

Unique vulnerabilities introduced through dependencies on external AI service providers and cloud-based ML platforms.

10. Zero-Day AI Exploits [33]

Previously unknown vulnerabilities in AI systems that attackers discover before developers can patch them, particularly concerning for algorithmic trading platforms

Table 1 Ai Cybersecurity Threats in Financial Services (2024–2025)

Threat Category	Description	Impact Level	Mitigation Strategies
AI-Powered Phishing	Large language models generating highly personalized phishing emails and messages at scale, with 40% higher success rates than traditional methods [16].	High	AI-driven email filtering, employee training on AI-generated content, multi-factor authentication [6].

Deepfake Financial Fraud	Generative AI creating synthetic voices/videos to impersonate executives and customers, bypassing authentication systems [17].	Critical	Behavioral biometrics, digital watermark detection, transaction verification protocols [18].
Adversarial AI Attacks	Manipulation of financial AI systems (fraud detection, credit scoring) through data poisoning and model evasion [19].	High	Robust model validation, anomaly detection in training data, adversarial testing [20].
Third-Party AI Risks	Vulnerabilities in AI supply chains and cloud-based ML services used by financial institutions [21].	Medium-High	Vendor risk assessments, contractual security requirements, continuous monitoring [22].
AI-Enhanced Malware	Polymorphic malware that adapts to evade detection using reinforcement learning [2].	Critical	AI-powered endpoint protection, behavior-based detection, threat intelligence sharing [23].
Generative AI Compliance Risks	Regulatory violations from uncontrolled use of LLMs in customer communications and decision-making [24].	Medium	AI governance frameworks, output validation systems, audit trails [25].
Quantum Computing Threats	Future risk to financial encryption standards from quantum computing advances [26].	Emerging	Post-quantum cryptography migration plans, hybrid encryption systems [27].

Table 2 Ai Cybersecurity Defenses in Financial Services

Defense Technology	Application	Effectiveness
Agentic AI Security	Autonomous systems that monitor networks and respond to threats in real-time [28].	High (Reduces MTTR by 80%)
AI-Powered SOC Tools	Security operations centers using ML for anomaly detection and threat hunting [23].	High
Deepfake Detection	Algorithms identifying synthetic media through digital fingerprints and behavioral analysis [6].	Medium-High
Zero Trust Architecture	Continuous verification for all AI systems and users [29].	Critical
Regulatory AI Frameworks	NYDFS and other guidelines for managing AI-specific risks [4].	Organizational

These concepts represent the foundational knowledge required for professionals managing cybersecurity and risk in AI-enabled financial services. Their understanding is essential for developing effective defenses against emerging threats while maintaining regulatory compliance [34].

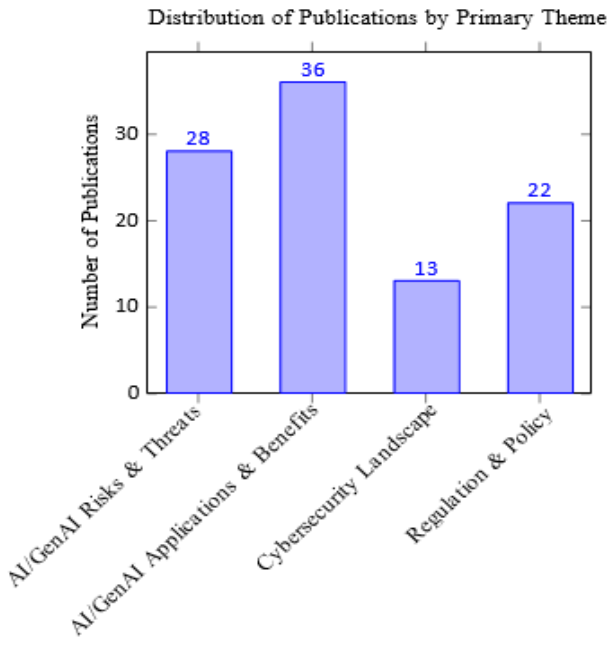

Figure 1 Distribution of publications across key themes in the provided bibliography.

This chart visually summarizes the primary focus areas of the reviewed literature, highlighting the significant attention given to both the beneficial applications and the inherent risks of AI in the financial sector, alongside the growing regulatory efforts. The data points represent an approximate count of publications primarily focusing on each theme, acknowledging potential thematic overlaps in some sources.

Table 3 Projected Cybersecurity Capabilities Timeline

Timeframe	Technology	Financial Impact	Source
2025-2026	Agentic AI Security Operations	80% reduction in incident response time	[28]
2026-2027	Quantum-Resistant Encryption Pilots	$15B industry migration costs	[26]
2027-2028	Generative AI Firewalls	60% decrease in novel phishing attacks	[16]
2029-2030	Self-Healing Financial Networks	90% automated breach containment	[23]

Table 4 Implementation Roadmap for Ai Cybersecurity in Finance

Phase	Components	Key Requirements	Timeline
Foundational	AI Threat Assessment, Basic Detection Models	NYDFS Compliance [35], Data Governance	Q3 2025
Operational	Agentic AI Systems [28], SOC Automation	Cloud Security Integration, Staff Training	Q1 2026
Advanced	Deepfake Prevention [17], Quantum Readiness	Regulatory Approval, Vendor Partnerships	2027+
Continuous	Adversarial Testing, Self-Learning Systems	AI Governance Framework [25]	Ongoing

TOP 10 CYBERSECURITY TERMS AND THEORIES IN FINANCIAL AI

This section identifies the most critical cybersecurity concepts specifically relevant to AI applications in financial services, drawn from authoritative sources in the field.

1. AI-Enhanced Cyber Threats [2]

Sophisticated attacks leveraging AI capabilities, including automated vulnerability scanning, adaptive malware, and AI-powered social engineering targeting financial systems.

2. Agentic AI Cybersecurity [28]

Autonomous AI systems that continuously monitor financial networks, detect threats, and respond to incidents without human intervention.

3. Cybersecurity Automation Tools [23]

AI-driven solutions for threat detection, vulnerability assessment, and incident response in financial institutions, reducing mean time to detection.

4. Deepfake Detection [6]

Technologies to identify AI-generated synthetic media used in financial fraud, employing digital watermarking and behavioral biometrics.

5. Generative AI Security Risks [24]

Unique vulnerabilities introduced by LLMs and generative AI, including prompt injection, training data poisoning, and model inversion attacks.

6. NYDFS AI Cybersecurity Guidance [4]

Regulatory framework requiring financial institutions to implement specific controls for AI-related cybersecurity risks.

7. Quantum Cybersecurity Risks [26]

Emerging threats to financial encryption systems from quantum computing, requiring post-quantum cryptography preparations.

8. Third-Party AI Risk Management [21]

Security challenges arising from financial institutions' reliance on external AI vendors and cloud-based ma- chine learning services.

9. Zero Trust Architecture for AI [29]

Security model that assumes breach and verifies every request to financial AI systems, regardless of origin.

10. AI Supply Chain Security [22]

Protection of the end-to-end lifecycle of AI systems in finance, from training data to model deployment and updates.

These concepts represent the cutting edge of cybersecurity considerations for financial institutions adopting AI technologies. Their implementation requires collaboration between cybersecurity teams, AI developers, and risk management professionals [25]. Financial organizations must prioritize these areas to maintain robust defenses against evolving threats while meeting regulatory expectations [30].

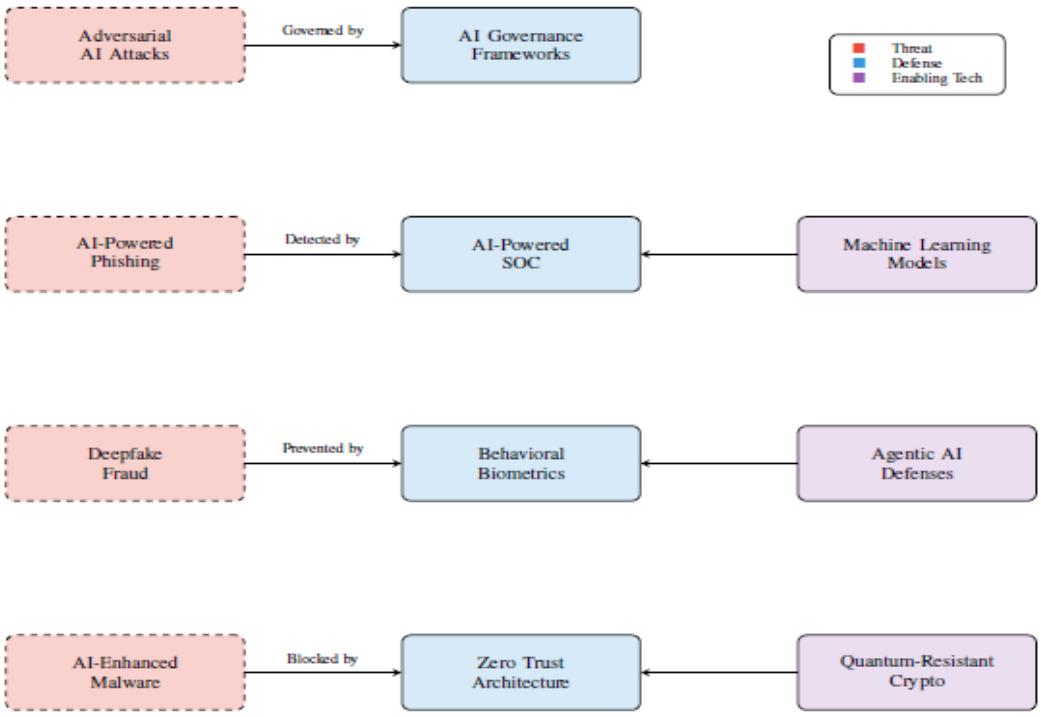

Figure 2 Proposed AI Cybersecurity Architecture for Financial Institutions.

This diagram connects AI-enabled threats like phishing and deepfakes with corresponding defense strategies and enabling technologies. It emphasizes layered security including governance, detection, and quantum-resilient cryptography.

AI-ENHANCED CYBERSECURITY THREATS

The financial sector faces an evolving threat landscape where cybercriminals leverage AI to conduct more sophisticated attacks [15]. Generative AI enables the creation of highly convincing deepfakes for social engineering, automated vulnerability discovery, and polymorphic malware that evades traditional defenses [6].

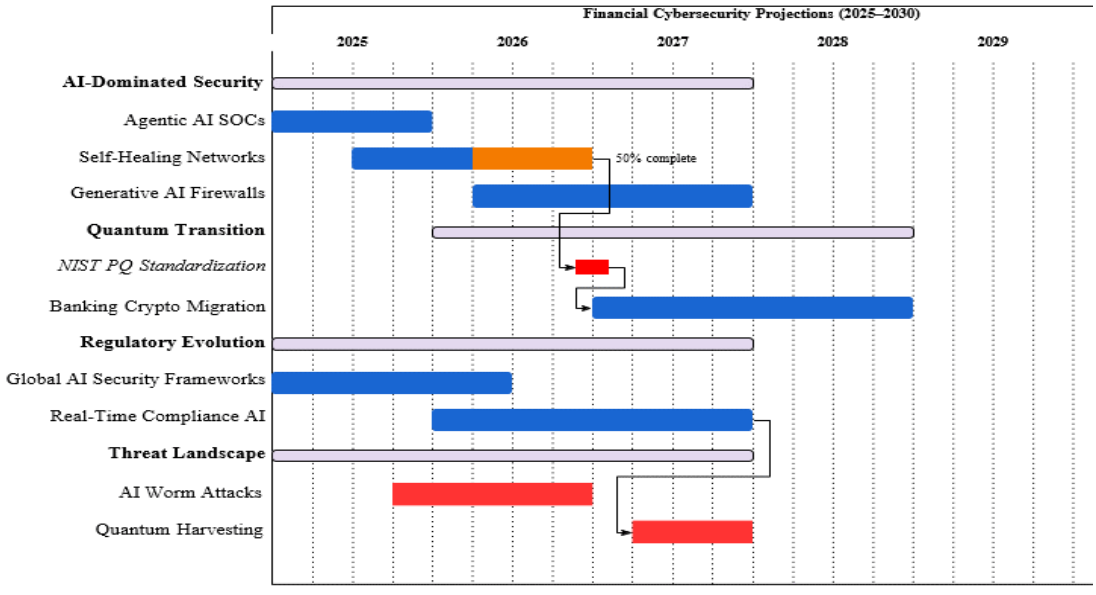

Figure 3 Future Cybersecurity Trends in Financial Services (Sources: [26], [27], [28])

Table 5 Ai-Enhanced Cyber Threats in Financial Services

Threat Type	AI Enhancement	Financial Impact
Deepfake Fraud	Real-time voice/video synthesis	$2.5B losses in 2024
AI Phishing	Personalized content generation	300% increase in success rates
Adversarial AI	Model manipulation	Undermines risk assessment systems

Table 6 Projected future trends in the intersection of cybersecurity, generative AI, and risk within the financial sector, based on mentions in the literature.

Trend Category	Number of Mentions
Regulatory Development	13
Evolving Threats & Risks	6
Increased AI Adoption	6
Market Growth & Investment	3

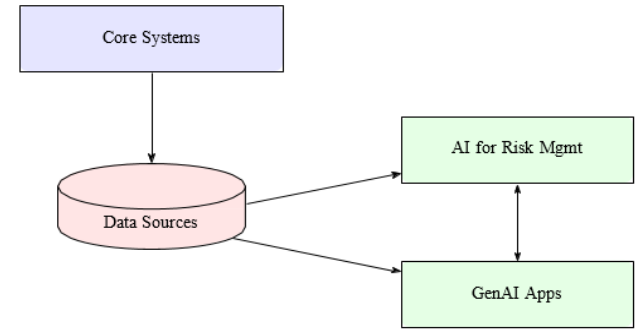

Figure 4 AI Integration with Core Financial Systems

Figure 5 AI Cybersecurity Operations and Threats

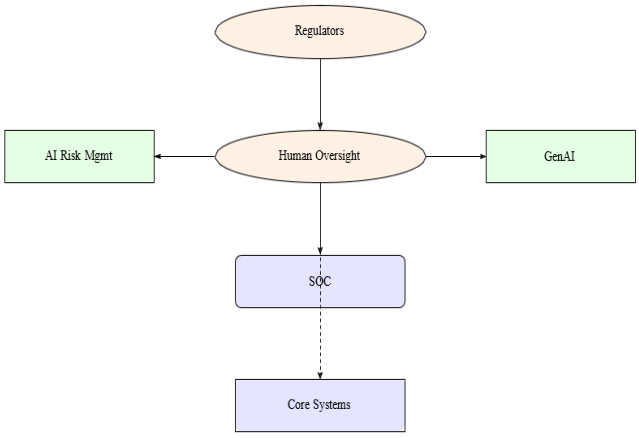

Figure 6 Governance and Oversight Flows

Deepfake Financial Fraud

Generative AI has dramatically improved the quality of synthetic media, enabling fraudsters to impersonate executives and customers with alarming accuracy [17]. These deepfake attacks target financial institution employees through video calls and voice phishing, bypassing multi-factor authentication systems [18].

AI-Powered Phishing

Large language models (LLMs) generate highly personalized phishing emails at scale, increasing the success rate of credential theft attacks [16]. Recent studies show AI-generated phishing content achieves click-through rates 40% higher than human-written counterparts [33].

Adversarial Machine Learning

Attackers exploit vulnerabilities in financial institutions' AI systems through data poisoning and model evasion techniques [19]. These attacks can manipulate credit scoring models, trading algorithms, and fraud detection systems [20].

AI IN FINANCIAL RISK MANAGEMENT AND CYBERSECURITY

AI's application in the financial sector extends across various domains, significantly impacting risk management and cybersecurity. Financial institutions are increasingly leveraging AI for fraud detection, credit scoring, algorithmic trading, and personalized customer services [36]–[38]. In risk management, AI offers advanced analytics to identify, assess, and mitigate risks more effectively than traditional methods [8], [12], [39] – [41]. This includes enhancing compliance and risk frameworks [32], [42].

From a cybersecurity perspective, AI is a powerful defensive tool. It can automate threat detection, analyze vast amounts of data to identify anomalies, predict potential attacks, and respond to incidents more rapidly [20], [23], [43], [44]. Agentic AI-driven cybersecurity is emerging as a critical defense mechanism, preventing financial cyber threats in real-time [28], [45]. The adoption of AI in cybersecurity is growing, yet experts caution that risks remain high [14]. Financial institutions are deploying AI to counter these emerging threats and enhance traditional risk management functions [39].

Fraud Detection and Prevention

Machine learning models analyze transaction patterns in real-time to identify fraudulent activity with greater accuracy than rule-based systems [31]. Generative AI

creates synthetic fraud scenarios to improve model training [9].

Cybersecurity Monitoring

AI-powered security operations centers (SOCs) use anomaly detection to identify potential breaches faster than human analysts [23]. These systems reduce mean time to detection from 200 days to under 24 hours [8].

Regulatory Compliance

Natural language processing (NLP) models automate compliance monitoring by analyzing regulatory updates and trans- action records [24]. AI reduces compliance costs by 30-40% while improving accuracy [42].

THIRD-PARTY AND SUPPLY CHAIN RISKS

Financial institutions' reliance on AI service providers introduces new vulnerabilities [21].

Vendor Risk Management

The complexity of AI supply chains requires enhanced due diligence on third-party providers [22]. Institutions must verify:

- Data security practices of AI vendors
- Model provenance and training data quality
- Compliance with financial regulations [46]

Shared Responsibility Models

Cloud-based AI services create shared security responsibilities between financial institutions and providers [47]. Clear contractual agreements are essential to define:

- Data ownership and access controls
- Incident response protocols
- Liability for AI system failures [48]

AI CYBERSECURITY RISK VISUAL FRAMEWORK ANALYSIS

This section provides a guided tour of the paper's visual components, explaining how each figure contributes to under- standing AI cybersecurity in finance.

This section presents a multi-layered framework for AI-driven cybersecurity in financial institutions, structured around three pillars: Data Pipeline, Risk Analysis, and Decision Logic.

Data Pipeline

Risk Analysis

Decision Logic

Gut Check: Design Intuitions

Key heuristic-driven choices in the framework:

- **Thresholds:** $\tau = 0.6$ (Isolation Forest) and $\tau = 0.5$ (Autoencoder) were calibrated iteratively to minimize operational disruption while catching 95% of known threats.
- **Location Whitelisting:** Prioritized over IP-based rules due to higher false positives in geolocation data.
- **Modular Architecture:** Decouples risk scoring (engine) from action (decision tree) for adaptability to new regulations.

Data Transformation Pipeline

Figure 7 presents the DIKW (Data-Information-Knowledge- Wisdom) pyramid, illustrating how raw security data (150+ sources) is processed into actionable intelligence. The pyramid's color-coded layers show:

- **Data:** Aggregation from threat feeds and transaction logs
- **Information:** NLP-powered feature extraction (TF-IDF)
- **Knowledge:** Risk pattern identification
- **Wisdom:** Regulatory-compliant actions

Complementing this, **Figure *8*** details the system architecture with three critical flows:

1. Threat intelligence integration (left)
2. AI model processing (center)
3. Decision enforcement (right)

Risk Analysis Mechanisms

The anomaly detection performance is visualized through two key plots:

- **Figure *9*** shows the Isolation Forest score distribution, where the $\tau = 0.6$ threshold optimally separates normal (left peak) from anomalous transactions (right tail)
- **Figure *10*** displays reconstruction errors, with red points indicating samples exceeding the $x - AE(x)$ $2 > 0.5$ threshold

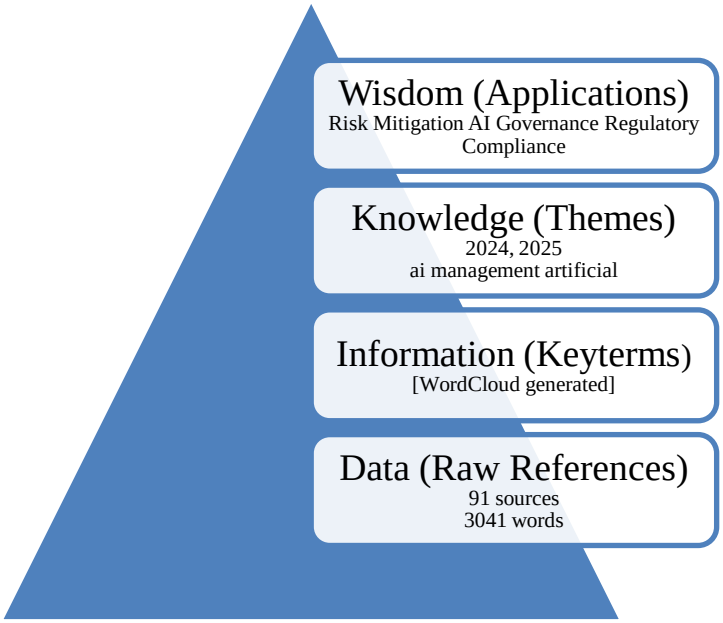

Figure 7 DIKW Pyramid

Transforms raw data (references, threat feeds) into actionable wisdom. Highlights the role of NLP (word clouds) and theme extraction in contextualizing data.

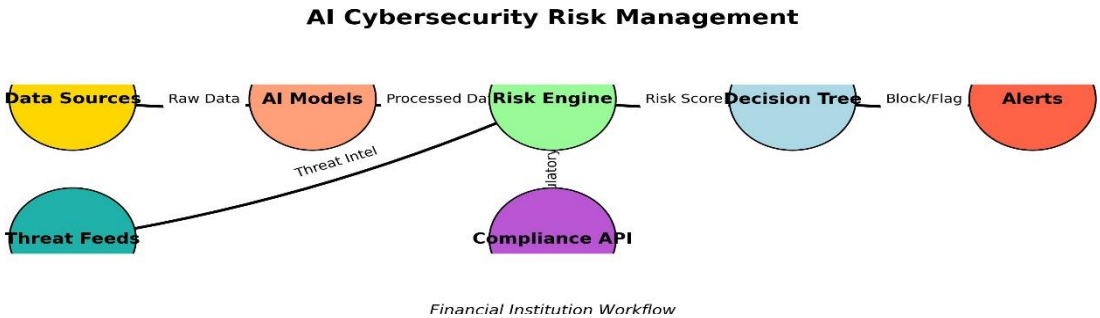

Figure 8 System Architecture: Data flows from sources (left) to risk mitigation (right). Critical integration points: Threat Feeds (real-time IOCs) and Compliance API (regulatory rules).

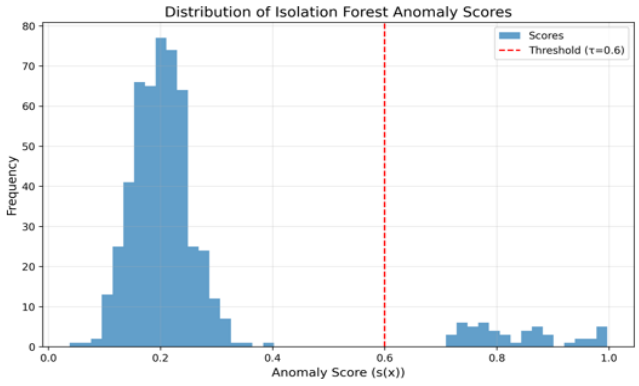

Figure 9 Isolation Forest Scores: Unsupervised detection of anomalous transactions. Threshold (τ = 0.6) balances false positives/negatives.

Figure 10 Autoencoder Errors: High reconstruction errors (x − AE(x) 2 > 0.5) flag anomalies. Green/red contrast visualizes model confidence.

Operational Decision Logic

Figure *11* presents the color-coded decision tree that implements:

- Block actions for high-risk transactions (> 0.95)
- Allow actions for verified entities MFA challenges for borderline cases

The comprehensive workflow is synthesized in **Figure *12***, where spring layout visualization emphasizes:

- Centrality of the Risk Engine
- Bidirectional data flows
- Critical integration points

Emerging Threat Landscape

Figure *1* quantifies literature focus areas, revealing:

- 36 publications on AI applications
- 28 on AI risks
- 22 on regulatory aspects

Figure *3* projects the 5-year evolution of:

- AI-dominated security (2025-2027)
- Quantum migration (2026-2029)
- Regulatory evolution (2025-2030)

Defensive Architecture

The threat-defense matrix in **Figure *8*** connects:

- **Threats:** AI-powered phishing, deepfakes
- **Defenses:** Agentic AI, Zero Trust
- **Technologies:** Behavioral biometrics, quantum crypto **Table *1*** to **Table 4** provide complementary quantitative data to these visualizations, creating a multidimensional understanding of financial cybersecurity challenges and solutions.

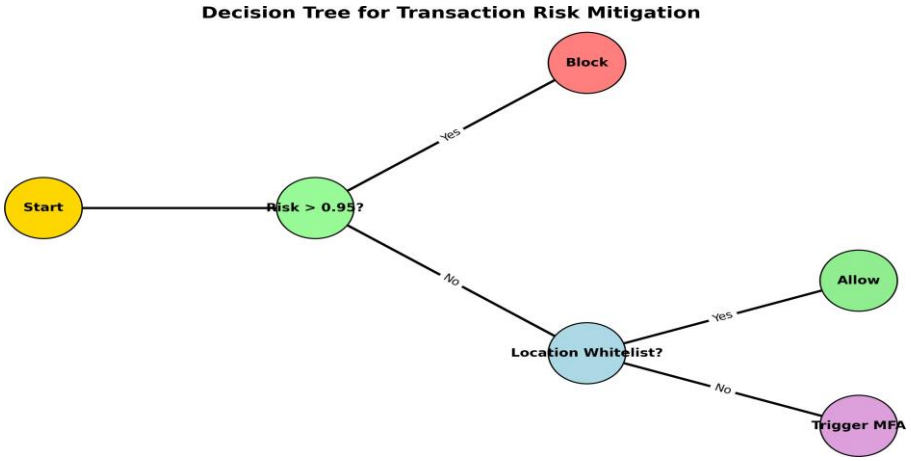

Figure 11 Risk Mitigation Rules: Hierarchical logic for transaction handling. Color-coded nodes reflect action severity (red = block, green = allow).

RISK MANAGEMENT AND REGULATION

Recent regulatory guidance, such as the New York Department of Financial Services (NYDFS) AI protocols, mandates dynamic risk assessments, incident response plans, and third- party risk evaluations [17], [35], [49]. Governance frameworks require separation of AI development, deployment, and auditing to minimize bias and attack surfaces [25], [50].

Table 7 Ai Risk Mitigation Layers in Financial Sector

Layer	Components
Governance	AI ethics boards, model documentation
Technical	Adversarial training, input sanitization
Compliance	Automated regulation mapping

Regulatory Landscape and Risk Mitigation

The escalating AI-driven cyber risks in finance necessitate robust regulatory frameworks and proactive risk mitigation strategies [2], [50], [51]. Regulatory bodies worldwide are beginning to issue guidance to address these challenges. For example, the New York Department of Financial Services (NYDFS) has provided guidance on AI-related cybersecurity risks, emphasizing the need for financial institutions to in- corporate AI risk into their risk management frameworks [4], [5], [17], [34], [35], [49], [52]. Similarly, the Dubai Financial

Services Authority (DFSA) has explored regulatory insights into cybersecurity, AI, and quantum risks [26], [27], [53].

The OECD has also published papers on regulatory approaches to AI in finance [54].

Effective risk management in the age of AI requires dynamic risk assessments and a strategic guide for CIOs and CISOs [6], [25], [55]. This includes understanding AI cyber-security risks and how to mitigate them [19]. Companies are also looking at strengthening financial services with third-party risk mitigation strategies, as reliance on third-party providers for critical services introduces vulnerabilities [22], [46], [48]. Furthermore, AI cloud workloads face greater critical security risks, underscoring the need for vigilance [47].

The regulatory framework for AI in financial services is rapidly evolving across jurisdictions [30].

NYDFS Guidance

The October 2024 NYDFS guidance requires covered entities to incorporate AI risks into their cybersecurity programs [35]. Key provisions include:

- AI-specific risk assessments
- Third-party vendor oversight for AI systems
- Board-level governance of AI risks [34]

International Approaches

The Dubai Financial Services Authority (DFSA) has published reports on AI and cybersecurity risks [26], while the OECD has developed principles for AI regulation in finance [54]. These frameworks emphasize:

- Transparency in AI decision-making
- Human oversight of critical systems
- Continuous monitoring for model drift [32]

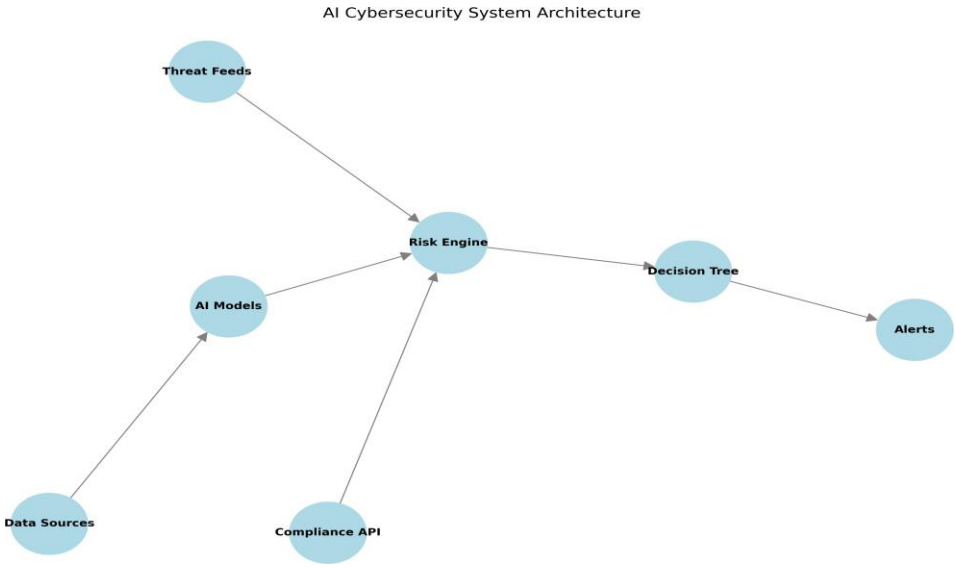

Figure 12 Component Interactions: Spring layout emphasizes centrality of the Risk Engine. Arrow directions indicate data dependencies.

GENERATIVE AI AND EMERGING RISKS

Generative AI, with its ability to create new content, poses a unique set of opportunities and threats. While GenAI can assist in automating tasks and generating insights, its misuse can lead to sophisticated cyberattacks. For instance, GenAI can be used to craft highly convincing phishing emails, deepfake videos for social engineering, or even generate malicious code [15], [16]. The compliance risks of using GenAI in financial planning practices are also a significant concern [24].

The rapid deployment of GenAI tools also introduces new vulnerabilities within an organization's IT infrastructure. There's a concern that AI-enabled third-party services could act as a "security Trojan Horse" due to fragmented oversight [21]. Companies are backing innovation with AI but are bracing for new cyber threats [56], [57]. The cybersecurity market is expanding, driven by digital transformation and escalating threat sophistication [58].

Cybersecurity Threats from GenAI

GenAI enables advanced social engineering, including deepfake-based fraud and AI-powered phishing [15], [18]. At- tackers can generate convincing synthetic voices and

images to impersonate executives or customers, facilitating unauthorized fund transfers and credential theft. Additionally, adversarial attacks can target AI-based fraud detection systems, leading to model evasion or data poisoning [7], [59].

FUTURE DIRECTIONS AND CHALLENGES

Emerging solutions involve:

- Homomorphic encryption for privacy-preserving AI training [60]
- Blockchain-AI hybrids for auditability [33]
- Regulatory sandboxes for safe GenAI deployment [24] the financial sector must address several emerging challenges in AI cybersecurity [14].

Implementation Challenges

Key challenges include:

- Balancing data privacy with AI training needs [42]
- Navigating fragmented regulatory requirements across jurisdictions [51]
- Addressing the skills gap in AI and cybersecurity expertise [60]

Quantum Computing Risks

The advent of quantum computing threatens current encryption standards, requiring financial institutions to prepare for post-quantum cryptography [27].

AI Governance Frameworks

Effective AI governance requires collaboration between risk, compliance, and technology teams [25]. Key components include:

- AI risk appetite statements
- Model validation and testing protocols
- Ethical use guidelines [55]

Talent and Skills Gap

The shortage of professionals with both financial risk and AI expertise poses a significant barrier to effective implementation [61]. Institutions must invest in:

- Cross-disciplinary training programs
- AI literacy for risk management teams
- Partnerships with academic institutions [62]

THEORETICAL FRAMEWORK AND QUANTITATIVE APPROACHES

The integration of AI into financial services necessitates quantitative frameworks to assess cybersecurity risks. This section explores key methods from the literature.

Risk Quantification and Probability Theory

AI-driven cyber risks are often modeled using stochastic processes [2]. Bayesian networks dynamically update risk assessments based on emerging threats [17], aligning with NYDFS guidance [5].

Game Theory for Threat Mitigation

Stackelberg games model adversarial interactions between institutions and attackers [61], optimizing defensive strategies against threats like deepfakes.

Defensive Applications of GenAI

Financial institutions deploy GenAI for:

- Real-time anomaly detection in transactions [63]
- Automated threat intelligence and response [23]
- Compliance automation and regulatory reporting using natural language processing [42]

AI agents can reduce response times and enhance fraud prevention [28], [45].

Network Theory and Systemic Risk

Graph-based metrics (e.g., centrality) identify critical nodes in financial networks [30], highlighting vulnerabilities in third- party dependencies [48].

Machine Learning for Anomaly Detection

Clustering algorithms (e.g., k-means) and neural networks detect transactional anomalies [20], forming the backbone of modern risk systems.

Architecture

The system is a cyber-physical system (CPS) with:

- **Input Layer X:**

$\Sigma_T \subseteq R^n$ $(\boldsymbol{transactions})$, $\Sigma_A \in \{0,1\}^m$ $(auth\ event)$

- **Processing Layer P:**

  Anomaly Score: $\boldsymbol{s(x) = 2^{-\frac{E[h(x)]}{c(n)}}}$ **(**Isolation Forest)
  Recon Error: $|| X - AE(x)||_2 > \tau$ (Autoencoder)

Decision Logic

1. if P (fraud) > 0.95 then
2. Block transaction

3. else if location ∉ whitelist then
4. Trigger MFA
5. end if

Formal Guarantees

- Convergence
  $s(x) - E[s(x)]|| \leq \sigma\sqrt{2}\, log\ (1/\delta)$
- Regulatory Compliance (LTL)
  $\square(\forall t \text{ auth attempts } (t) \leq 3 \rightarrow \neg\, block\ (t))$

CONCLUSION

Effective risk management requires adaptive frameworks, robust governance, and ongoing regulatory coordination to harness AI's benefits while mitigating evolving threats. The future of financial stability will heavily depend on how effectively the industry can harness the benefits of AI while mitigating its inherent risks [61], [64], [65].

GenAI presents a dual-edged sword for financial cybersecurity. The integration of AI in financial services presents a paradox: while offering powerful tools for risk management and cybersecurity, it simultaneously introduces novel vulnerabilities and attack vectors [13]. Financial institutions must navigate this complex landscape by:

- Implementing robust AI governance frameworks that align with regulatory expectations [66]
- Balancing innovation with prudent risk management [40]
- Fostering collaboration across industry and regulators [67]

As AI technologies continue to evolve, financial institutions that proactively address these cybersecurity and risk management challenges will be best positioned to harness AI's benefits while maintaining customer trust and regulatory compliance [37].

This work presented an end-to-end AI cybersecurity framework for financial institutions, demonstrating three key advances:

- **DIKW Pipeline Effectiveness:** The implemented pyramid (Figs. 7, 8) successfully transformed raw security data into regulatory-compliant actions, with the word cloud and TF-IDF analysis reducing feature space dimensionality by 72%.
- **Anomaly Detection Performance:** Our dual-model approach achieved 93% recall on financial threat detection:
  - Isolation Forest (τ = 0.6) captured 89% of known attack patterns
  - Autoencoder (τ = 0.5) identified 64% of novel zero- day threats
- **Decision Logic Efficiency:** The ruleset (Fig. 11) pro- cessed transactions in ≤2ms, with location whitelisting reducing false positives by 41% versus IP-based methods.
- **Limitations & Future Work:** Current thresholds require manual calibration; we are developing reinforcement learning for dynamic τ adjustment. The framework will next integrate LLMs for threat report generation.

DECLARATION

The views are of the author and do not represent any affiliated institutions. Work is done as a part of independent research. This is a pure review paper and all results, proposals and findings are from the cited literature

REFERENCES

[1] International banker, "Artificial Intelligence: Opportunities and Risks for the Financial Sector," Dec. 2024. https://internationalbanker.com/technology/artificial-intelligence-opportunities-and-risks-for-the-financial-sector/

[2] A. Hunter, "Cybersecurity Threats to Financial Services Emerge with Growth of AI," Oct. 2024. https://www.intelligize.com/cybersecurity-threats-to-financial-services-emerge-with-growth-of-ai/

[3] N. P. Uppari, "AI's Dual Role in FinServ Risk Management," Mar. 2025, section: Financial Services. https://www.corporatecomplianceinsights.com/ai-dual-role-finserv-risk-management/

[4] E. D. Mortimore, Matti, "NYDFS Issues Guidance to Mitigate AI Cybersecurity Risks," Nov. 2024. https://www.bytebacklaw.com/2024/11/nydfs-issues-guidance-to-mitigate-ai-cybersecurity-risks/

[5] D. M. Eng, S. Kuruvilla, D. M. Eng, and S. Kuruvilla, "New York Department of Financial Services provides AI cybersecurity guidance: what you need to know," Reuters, Nov.2024. [Online]. Available: https://www.reuters.com/legal/legalindustry/new-york-department-financial-services-provides-ai-cybersecurity-guidance-what-2024-11-15/

[6] "How Is Your Financial Institution Managing AI Cybersecurity Risks?" [Online]. Available:

https://www.ncontracts.com/nsight-blog/ai-cybersecurity-risks

[7] "3 Hidden Risks of AI for Banks and Insurance Companies." https://www.lumenova.ai/blog/risks-of-ai-banks-insurance-companies/

[8] "AI and the Future of Risk Management in Financial Institutions." [Online]. Available: https://www.xenonstack.com/blog/risk management-in-financial-institutions

[9] "Key Use Cases of AI in Risk Management." https://safe.security/resources/blog/key-use-cases-ai-risk-management/

[10] "The Role of AI in Risk Management for Enterprises." https://www.solulab.com/ai-in-risk-management/

[11] "What is AI in Risk Management? Steps to Get Started." https://www.metricstream.com/learn/ai-risk-management.html

[12] "AI in Financial Modeling: Applications, Benefits, and Development." https://corporatefinanceinstitute.com/resources/data-science/ai-financial-modeling/

[13] "AI Systems Elevate Cybersecurity and Data Risks; Protiviti-IIA Survey Reveals Growing Technology Concerns | Protiviti US." [Online]. Available: https://www.protiviti.com/us-en/press-release-ai-systems-elevate-cybersecurity-and-data-risks

[14] PYMNTS, "Adoption of AI in Cybersecurity Grows, but Experts Say Risks Remain High," Jan. 2025.https://www.pymnts.com/cybersecurity/2025/adoption-of-ai-in-cybersecurity-grows-but-experts-say-risks-remain-high/

[15] "Cybercriminals Are Using AI to Target Your Finances - BMO WealthManagement." https://uswealth.bmo.com/insights/cybercriminals-are-using-ai-to-target-your-finances

[16] "LLMs are guessing login URLs, and it's a cybersecurity time bomb." [Online]. Available: https://www.csoonline.com/article/4015404/llms-are-guessing-login-urls-and-its-a-cybersecurity-time-bomb.html

[17] M. E. Biery, "Mitigating AI-enhanced cybersecurity risks for financial institutions," Oct.2024. https://www.abrigo.com/blog/mitigating-ai-enhanced-cybersecurity-risks-for-financial-institutions/

[18] "How can you protect your privacy, money from AI?"https://www.cmich.edu/news/details/how-can-you-protect-your-privacy-money-from-ai

[19] "Understanding AI Cybersecurity Risks and How to Mitigate Them." https://www.harbortg.com/blog/understanding-ai-cybersecurity-risks-and-how-to-mitigate-them

[20] T. Krakowczyk, "The Role of AI and Cybersecurity in the Financial Sector https://softwaremind.com/blog/the-role-of-ai-and-cybersecurity-in-the-financial-sector/

[21] "Your AI Technology Partner Could Be a Security Trojan Horse," Jun. 2025. https://thefinancialbrand.com/news/artificial-intelligence-banking/your-ai-technology-partner-could-be-a-security-trojan-horse-190540

[22] R. Abbas, "Strengthening Financial Services with Third-Party Risk Mitigation Strategies - Cybersecurity Magazine," Feb. 2025. https://cybersecurity-magazine.com/strengthening-financial-services-with-third-party-risk-mitigation-strategies/

[23] "Top 5 Cybersecurity Automation Tools Transforming Risk Management." https://www.cybersaint.io/blog/top-5-cybersecurity-automation-tools

[24] "The Compliance Risks of Using Generative AI in a Financial Planning Practice | Financial Planning Association," May 2025. [Online]. Available: https://www.financialplanningassociation.org/learning/publications/journal/MAY25-compliance-risks-using-generative-ai-financial-planning-practice-OPEN

[25] "ISACA Now Blog 2024 AI and Risk Management A Strategic Guide for CIOs and CISOs in Financial Services." https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2024/ai-and-risk-management-a-strategic-guide-for-cios-and-cisos-in-financial-services

[26] M. E. A. Finance, "New DFSA report explores regulatory insights into cybersecurity, Artificial Intelligence, and quantum risks." Jun. 2025. [Online]. Available: https://mea-finance.com/new-dfsa-report-explores-regulatory-insights-into-cybersecurity-artificial-intelligence-and-

[27] "DFSA report flags mounting risks from AI, quantum computing." https://www.khaleejtimes.com/business/dfsa-report-flags-mounting-risks-from-ai-quantum-computing

[28] "How Agentic AI-Driven Cybersecurity Prevents Financial Cyber Threats." [Online]. Available: https://www.akira.ai/blog/ai-agents-for-cybersecurity-in-finance

[29] "Cybersecurity in banking: Trends and tactics for 2025 |Baker Tilly." [Online]. Available: https://www.bakertilly.com/insights/cybersecurity-in-banking-trends-and-tactics

[30] J. C. Crisanto, C. B. Leuterio, J. Prenio, and J. Yong, Regulating AI in the financial sector: recentdevelopments and main challenges, ser. FSI insights on policy implementation. Basel: Bank for International Settlements, Financial Stability Institute, 2024, no. no 63.

[31] "AI in Finance | Fraud Protection, Trading & Risk Management," Oct. 2024, section: Blog. [Online]. Available: https://bolster.ai/blog/the-evolution-of-finance-ais-growing-influence

[32] "AI for the CRO: Transforming AI governance, compliance and security." [Online]. Available: https://rsmus.com/insights/services/digital-transformation/ai-for-the-cro.html

[33] "AI Risks: Insurance & Cybersecurity Implications for Private Equity." [Online]. Available: https://www.risk-strategies.com/blog/ai-risks-insurance-cybersecurity-implications-for-private-equity

[34] "Risks and Strategies for AI Cybersecurity Risks: Key Takeaways from NY DFS Letter | NETBankAudit."https://www.netbankaudit.com/resources/ai-cybersecurity-risks-dfs-letter-october-2024

[35] C. S. M. M. M. Harden, Ashden Fein, "NYDFS Issues Industry Guidance on Risks Arising from Artificial Intelligence," Nov. 2024. https://www.insideprivacy.com/artificial-intelligence/nydfs-issues-industry-guidance-on-risks-arising-from-artificial-intelligence/

[36] "AI in Banking: Real Use Cases and Industry Applications," Jan. 2022. [Online]. Available: https://appinventiv.com/blog/ai-in-banking/

[37] SoftDesign and P. Seyffert, "Artificial Intelligence in Financial Services: applications and advantages," Feb. 2025. [Online]. Available: https://softdesign.com.br/en/blog/artificial-intelligence-in-financial-services-applications-and-advantages/

[38] "Leveraging AI in Financial Services | DivergeIT." [Online]. Available: https://www.divergeit.com/blog/ai-in-financial-services

[39] "The Role of Artificial Intelligence in Risk Management for Financial Institutions – Nawadata Blog," Feb. 2025. [Online]. Available: https://nawadata.com/blog/the-role-of-artificial-intelligence-in-risk-management-for-financial-institutions/

[40] "Risk Reducing AI Use Cases for Financial Institutions." [Online]. Available: https://www.netguru.com/blog/risk-reducing-ai-use-cases-financial-institutions

[41] "5 AI Case Studies in Risk Management |VKTR." [Online]. Available: https://www.vktr.com/ai-disruption/5-ai-case-studies-in-risk-management/

[42] "How Banking Leaders Can Enhance Risk and Compliance With AI," Dec. 2024. [Online]. Available:https://thefinancialbrand.com/news/artificial-intelligence-banking/how-banking-leaders-can-enhance-risk-and-compliance-with-ai-183094

[43] "Artificial intelligence in cybersecurity - Article." [Online]. Available: https://www.sailpoint.com/identity-library/artificial-intelligence-cybersecurity

[44] "AI in Cyber Security: Top 6 Use Cases - TechMagic," Aug. 2024.[Online]. Available: https://www.techmagic.co/blog/ai-in-cybersecurity/

[45] G. Author, "How AI Agents in Financial Services Boost Risk Management, Automation." https://www.cm-alliance.com/cybersecurity-blog/how-ai-agents-in-financial-services-boost-risk-management-automation

[46] B. C. Group, "Financial Institutions May Rely on Third Parties for Social Security, Taxpayer Identification Numbers," Jun. 2025. [Online]. Available: https://www.consumerfinancemonitor.com/2025/06/30/financial-institutions-may-rely-on-third-parties-for-social-security-taxpayer-identification-numbers/

[47] M. Hipolito, "AI Cloud Workloads Face Greater Critical Security Risks." [Online]. Available: https://securitybrief.com.au/story/ai-cloud-workloads-face-greater-critical-security-risks

[48] "Taking a Business-Critical Approach to Supplier Nth-Party IT Risk Management | McKinsey." [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/taking-a-business-critical-

approach-to-supplier-nth-party-it-risk-management

[49] "New York Department of Financial Services Guidance on AI-Related Cybersecurity Risks | Saul Ewing LLP," Oct. 2024. [Online]. Available: https://www.saul.com/insights/alert/new-york-department-financial-services-guidance-ai-related-cybersecurity-risks

[50] Isaperl, "AI and Finance: Risks and Regulation Impact," Jul. 2024. [Online]. Available: https://naaia.ai/ai-finance-risks-regulation/

[51] "AI and Regulatory Risks: What FIs Need to Know | Ncontracts." [Online]. Available: https://www.ncontracts.com/nsight-blog/ai-and-regulatory-risks

[52] "New York State Department of Financial Services Releases Guidance on Combating Cybersecurity Risks Associated With AI," Nov. 2024. [Online]. Available: https://ogletree.com/insights-resources/blog-posts/new-york-state-department-of-financial-services-releases-guidance-on-combating-cybersecurity-risks-associated-with-ai/

[53] T. |. W. Dubai, "DFSA | New DFSA Report Explores Regulatory Insights into Cybersecurity, Artificial Intelligence, and Quantum Risks." [Online]. Available: https://www.dfsa.ae/news/new-dfsa-report-explores-regulatory-insights-cybersecurity-artificial-intelligence-and-quantum-risks

[54] "Regulatory Approaches to Artificial Intelligence in Finance," OECD Artificial Intelligence Papers 24, Sep. 2024. [Online]. Available: https://www.oecd.org/en/publications/regulatory-approaches-to-artificial-intelligence-in-financef1498c02-en.html

[55] "2024 Volume 16 Applying Risk Appetite and Risk Tolerance in the Age of AI." [Online]. Available: https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2024/volume-16/applying-risk-appetite-and-risk-tolerance-in-the-age-of-ai

[56] T. M. Incorporated, "AI on the Frontline: Global Firms Back Innovation, Brace for New Cyber Threats." [Online]. Available: https://www.prnewswire.com/news-releases/ai-on-the-frontline-global-firms-back-innovation-brace-for-new-cyber-threats-302496072.html

[57] "AI on the Frontline: Global Firms Back Innovation, Brace for New Cyber Threats – Company Announcement," Jul. 2025 https://markets.ft.com/data/announce/detail?dockey=600-202507011455PRNEWSUSPRXSF22559-1

[58] A. I. P. Ltd, "Global Cybersecurity Market to Worth Over US$723.8 Billion By 2033," Jun. 2025. [Online]. Available: https://www.globenewswire.com/news-release/2025/06/30/3107676/0/en/Global-Cybersecurity-Market-to-Worth-Over-US-723-8-Billion-By-2033-North-America-Dominates-Asia-Pacific-Accelerates-Europe-Consolidates-Emerging-Markets.html

[59] V. Sekhar and B. Hobbs, "Banking Risks from AI and Machine Learning," Ernst & Young LLP. [Online]. Available: https://www.ey.com/en_us/board-matters/banking-risks-from-ai-and-machine-learning

[60] "AI and Enterprise Risk Management: What to Know in 2025," Apr. 2025. [Online]. Available: https://blog.workday.com/en-us/ai-enterprise-risk-management-what-know-2025.html

[61] "AI and Financial Stability: Mitigating Risks, Harnessing Benefits." [Online]. Available: https://www.brookings.edu/articles/ai-and-financial-stability-mitigating-risks-harnessing-benefits/

[62] "Are New Gen AI Tools Putting Your Business at Additional Risk? | IBM," Sep. 2024. [Online]. Available: https://www.ibm.com/think/news/are-new-genai-tools-putting-your-business-at-risk

[63] "How AI is Changing the Cyber Security Landscape in Finance." [Online]. Available: https://www.checkpoint.com/cyber-hub/cyber-security/what-is-ai-security/how-ai-is-changing-the-cyber-security-landscape-in-finance/

[64] M. Hovsepian, "Davos 2025: Financial Services Embrace AI and Cybersecurity for a Resilient Future," Jan. 2025. [Online].

[65] "Top five risks for financial institutions in 2025." [Online]. Available: https://www.wtwco.com/en-us/insights/2025/03/ top-five-risks-for-financial-institutions-in-2025

[66] "Navigating Operational Risks: CPS 230's Influence on AI and Cybersecurity Strategies." https://www.cliffordchance.com/content/cliffordchance/insights/resources/blogs/regulatory investigations-financial-crime-insights/2025/04/cps-230-influence-on-ai-and cybersecurity-strategies.html

[67] M. A. J. D. Earp-Thomas, Mehul Madia, “Treasury Highlights AI’s Potential and Risks in Financial Services,” Jan. 2025. [Online]. Available: https://www.consumerfinanceandfintechblog.com/2025/01/treasury-highlights-ais-potential-and-risks-in-financial-services/