MUSCAT INTERNATIONAL FORUM FOR
RISK MANAGEMENT IN BANKS
& FINANCIAL INSTITUTIONS | 3rd EDITION

6 - 7 OCTOBER
MUSCAT | 2025
OMAN

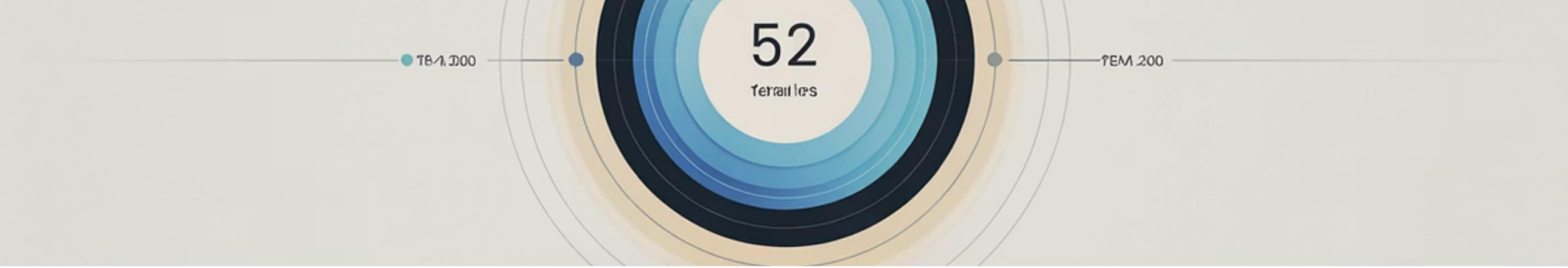
IN
COLLABORATION
WITH

Union of Arab Banks

CENTRAL BANK OF OMAN

Innovation and Digitalization in Risk Management

Prof. Samir El-Masri
President of Arab Society for Digital Transformation
Chairman of Digitalization



1. The Fintech Revolution and Emerging Cyber Threats

Financial technology reshapes the banking landscape with new opportunities emerge alongside unprecedented cyber risks:

- Fintech innovations are transforming the industry
- Security challenges that require immediate attention from risk management professionals

Largest Companies by Marketcap

Companies: **10,645** total market cap: **$133.084 T**

Rank by | Market Cap | Earnings | Revenue | Employees | P/E ratio | Dividend % | Market Cap gain | More +

	Rank	Name	Market Cap	Price	Today	Price (30 days)	Country
☆	1	NVIDIA NVDA	$4.567 T	$187.62	▼ 0.70%		USA
☆	2	Microsoft MSFT	$3.845 T	$517.35	▲ 0.31%		USA
☆	3	Apple AAPL	$3.829 T	$258.02	▲ 0.35%		USA
☆	4	Alphabet (Google) GOOG	$2.975 T	$246.45	▲ 0.01%		USA
☆	5	Amazon AMZN	$2.341 T	$219.51	▼ 1.30%		USA
☆	6	Meta Platforms (Facebook) META	$1.785 T	$710.56	▼ 2.27%		USA
☆	7	Saudi Aramco 2222.SR	$1.598 T	$6.61	▲ 0.16%		S. Arabia
☆	8	Broadcom AVGO	$1.597 T	$338.37	▲ 0.06%		USA
☆	▲1 9	TSMC TSM	$1.515 T	$292.19	▲ 1.42%		Taiwan
☆	▼1 10	Tesla TSLA	$1.429 T	$429.83	▼ 1.42%		USA

Big Techs

Apple $383.8 billion > 60 countries

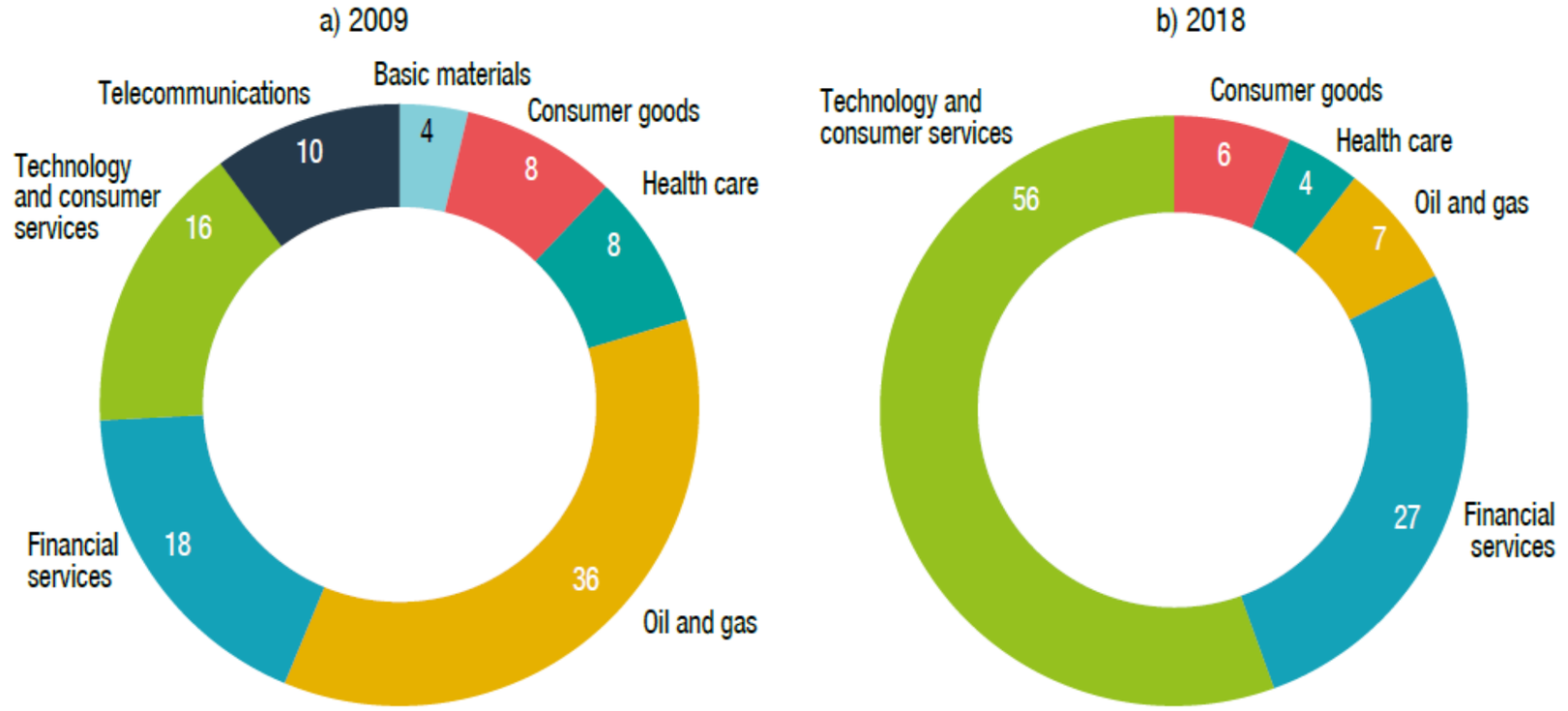
Amazon $638 billion > 75 Countries

Samsung Revenue > Kuwait's economy

Apple > $3 trillion
NVIDIA > $4 trillion
Microsoft > $3 trillion

UNCTAD: United Nations Conference on Trade and Development

Figure I.16. World's top 20 companies by market capitalization, by sector, 2009 versus 2018
(Per cent)

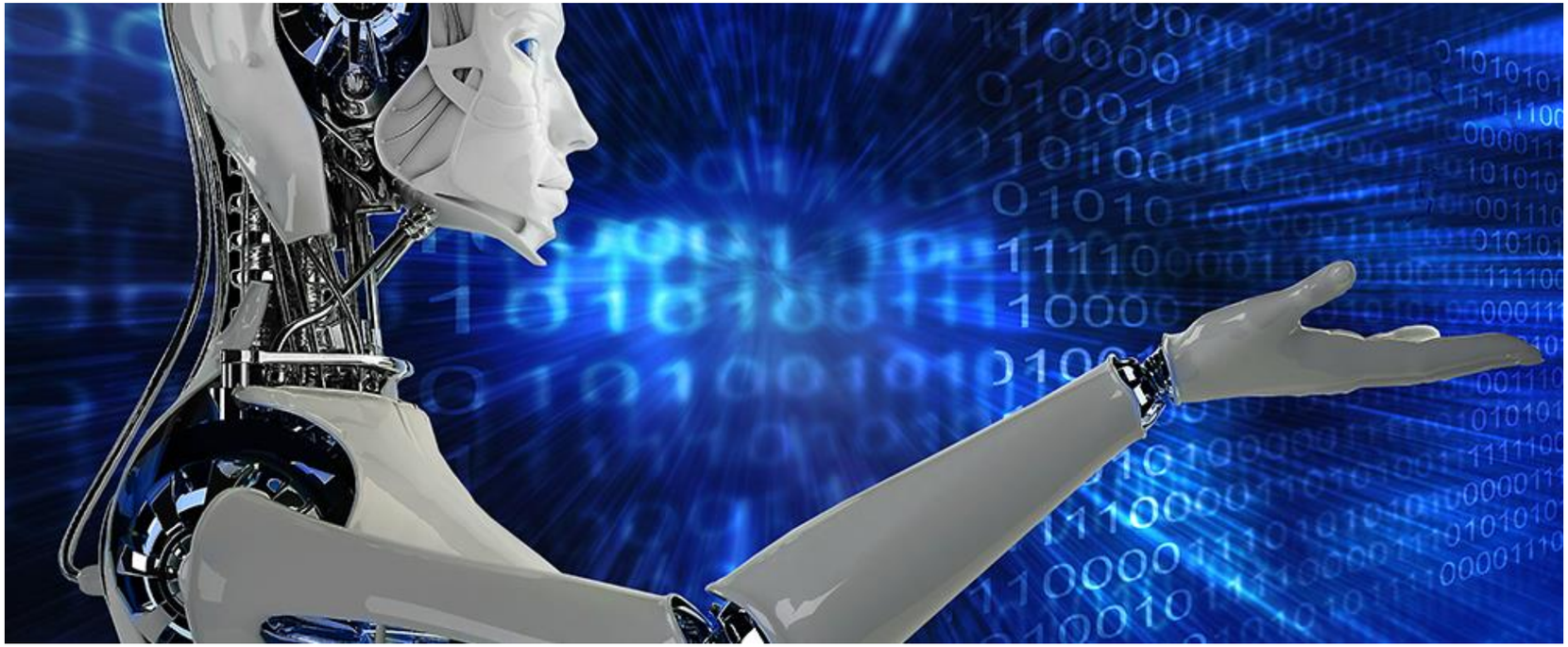


Source: UNCTAD, based on PwC, 2018b.

AI Technologies will generate $15.7 trillion by 2030

Generative AI will generate $4.4 trillion

FinTech will generate $1.5 trillion



Fintech's Rapid Rise: Promise and Peril

21%

YoY Growth

Fintech revenues surged in 2024, significantly outpacing traditional finance sector growth rates

60%

Revenue Concentration

Market share generated by fewer than 100 scaled fintech players globally

100+

Key Players

Dominant fintech companies driving sector transformation and innovation

The fintech sector's explosive growth represents both unprecedented opportunity and significant risk. While these companies deliver innovative solutions that enhance customer experience and operational efficiency, their rapid expansion introduces new vulnerabilities that traditional risk management frameworks may not adequately address. Financial institutions must carefully balance embracing fintech innovation with maintaining robust security and compliance standards.

The Evolving Cyber Threat Landscape

Traditional Security Compromised

Device fingerprinting and behavioral biometrics, once considered cutting-edge security measures, have become widely compromised. Cybercriminals now possess sophisticated tools to bypass these authentication methods, forcing institutions to constantly evolve their security strategies.

- Advanced spoofing techniques
- Behavioral pattern mimicry
- Device emulation tools

Democratized Cybercrime

Dark web marketplaces have transformed cybercrime from elite hacker activities to accessible criminal services. The FBI's 2024 shutdown of a prominent dark web marketplace revealed how easily sophisticated fraud tools can be purchased and deployed by novice criminals.

- Fraud-as-a-Service platforms
- Automated attack tools
- Credential marketplaces

Fintech and Banks: Blurring Lines, Blurring Risks

01

Charter Pursuit

Leading fintechs are actively pursuing traditional bank charters to navigate increasingly complex regulatory requirements and gain direct access to payment systems.

02

Strategic Partnerships

Traditional banks are forming deeper partnerships with fintech companies, creating interconnected ecosystems that share both operational efficiencies and systemic risks.

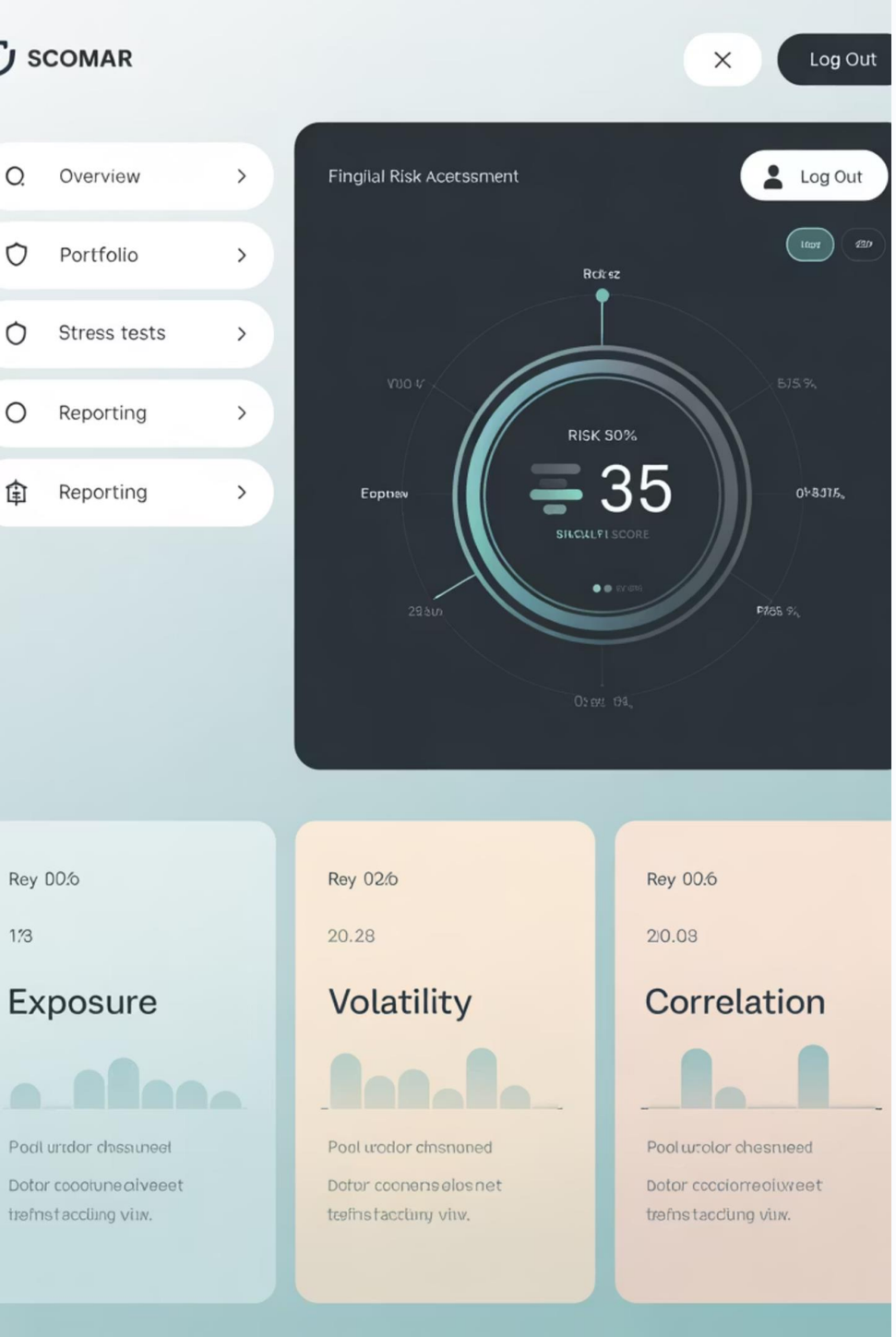
03

Regulatory Oversight

Regulators now demand clear governance structures and comprehensive risk oversight frameworks for these hybrid banking-fintech models to ensure consumer protection and systemic stability.

2. Open Banking Risks and Third-Party Dependencies

Open banking initiatives promise to revolutionize financial services through enhanced competition and innovation. However, this openness creates new vulnerabilities as banks must carefully manage data privacy, third-party dependencies, and the complex web of relationships that define the modern financial ecosystem.



Open Banking: Unlocking Innovation, Exposing Data Risks

API Innovation

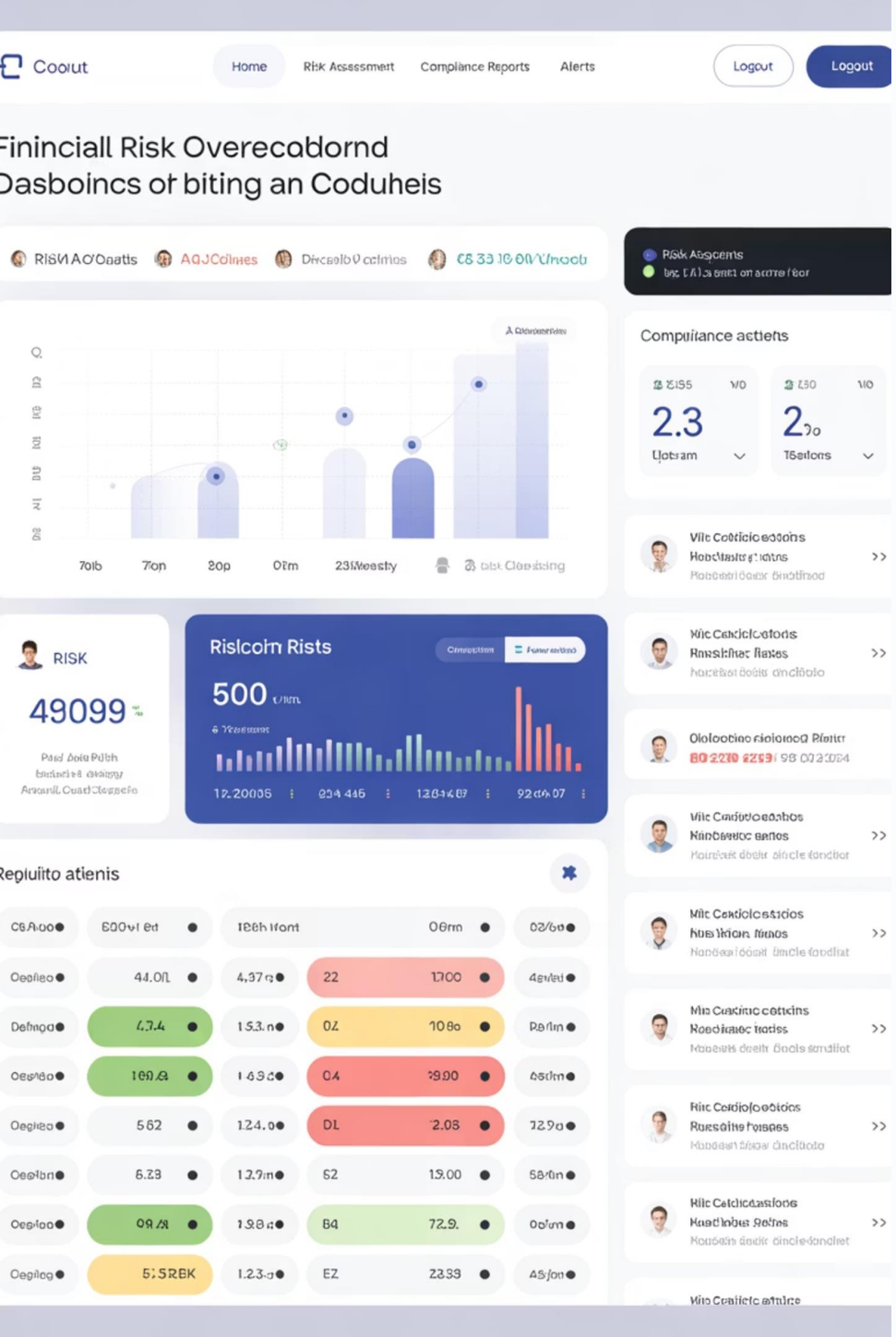
Open APIs enable seamless data sharing between financial institutions and third-party providers, creating unprecedented opportunities for personalized financial services and streamlined customer experiences.

Privacy Challenges

Increased data sharing amplifies exposure to potential breaches, requiring sophisticated privacy protection mechanisms and transparent customer consent management processes.

Dependency Risks

Banks must carefully manage concentration risks and operational dependencies on fintech partners to maintain service continuity and regulatory compliance.



Regulatory Spotlight on Bank-Fintech Relationships

Regulatory Classification

U.S. regulators are treating bank-fintech relationships as formal business arrangements rather than informal partnerships, requiring documented agreements and clear accountability structures.

FDIC Requirements

The FDIC's proposed rules mandate that banks maintain direct access to custodial account data, ensuring regulatory oversight even in partnership arrangements.

Key Compliance Requirement: Heightened due diligence and ongoing oversight are now mandatory for all fintech investments and partnerships, with regular reporting requirements to regulatory authorities.

Case Study: Regulatory Actions Against Fintechs

1 CFPB Enforcement Actions

The Consumer Financial Protection Bureau has increased scrutiny of fintech practices, particularly focusing on deceptive marketing practices and inadequate consumer disclosures.

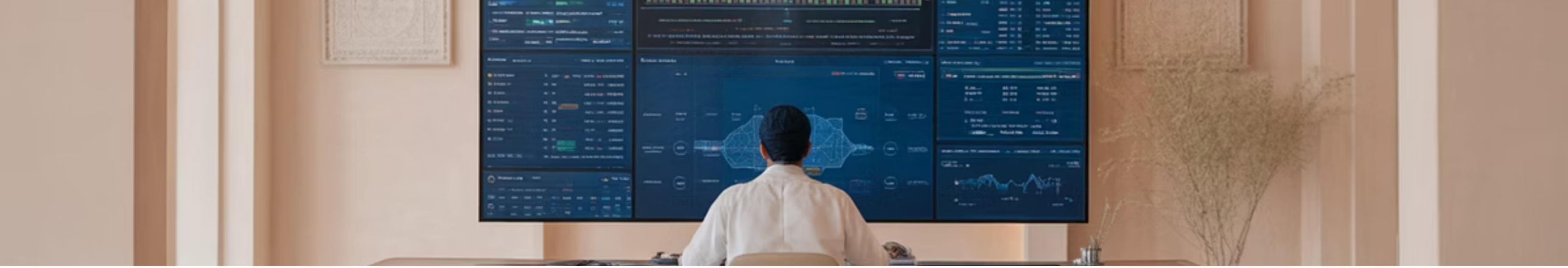
2 FTC Intervention

Federal Trade Commission actions in 2024 highlighted risks associated with data privacy violations and unfair business practices in the fintech sector.

3 Consent Orders

Recent consent orders emphasize the critical importance of robust AML programs, cybersecurity measures, and comprehensive third-party risk management frameworks.

These regulatory actions demonstrate that fintechs must carefully balance innovation speed with compliance rigor to maintain sustainable growth and avoid costly enforcement actions that can damage reputation and market position.



The Next Frontier

3. AI-Driven Risk Management

Opportunities and Challenges

Artificial intelligence is revolutionizing risk management in financial services, offering unprecedented capabilities in fraud detection, credit assessment, and compliance monitoring. However, AI also introduces new risks that institutions must carefully navigate to realize its full potential while maintaining security and fairness.

AI Transforming Fraud Detection and Credit Scoring

Artificial intelligence is fundamentally reshaping how financial institutions approach two critical areas: fraud detection and credit scoring. By leveraging advanced algorithms and machine learning, AI offers capabilities that far surpass traditional methods, leading to more secure transactions and equitable access to financial services.

Real-Time Analysis

AI systems analyze thousands of signals simultaneously, reducing fraud investigation times from hours to milliseconds. This includes processing multiple data streams, identifying subtle behavioral patterns, cross-referencing transaction histories, and analyzing device fingerprints to detect anomalies and flag suspicious activities instantaneously.

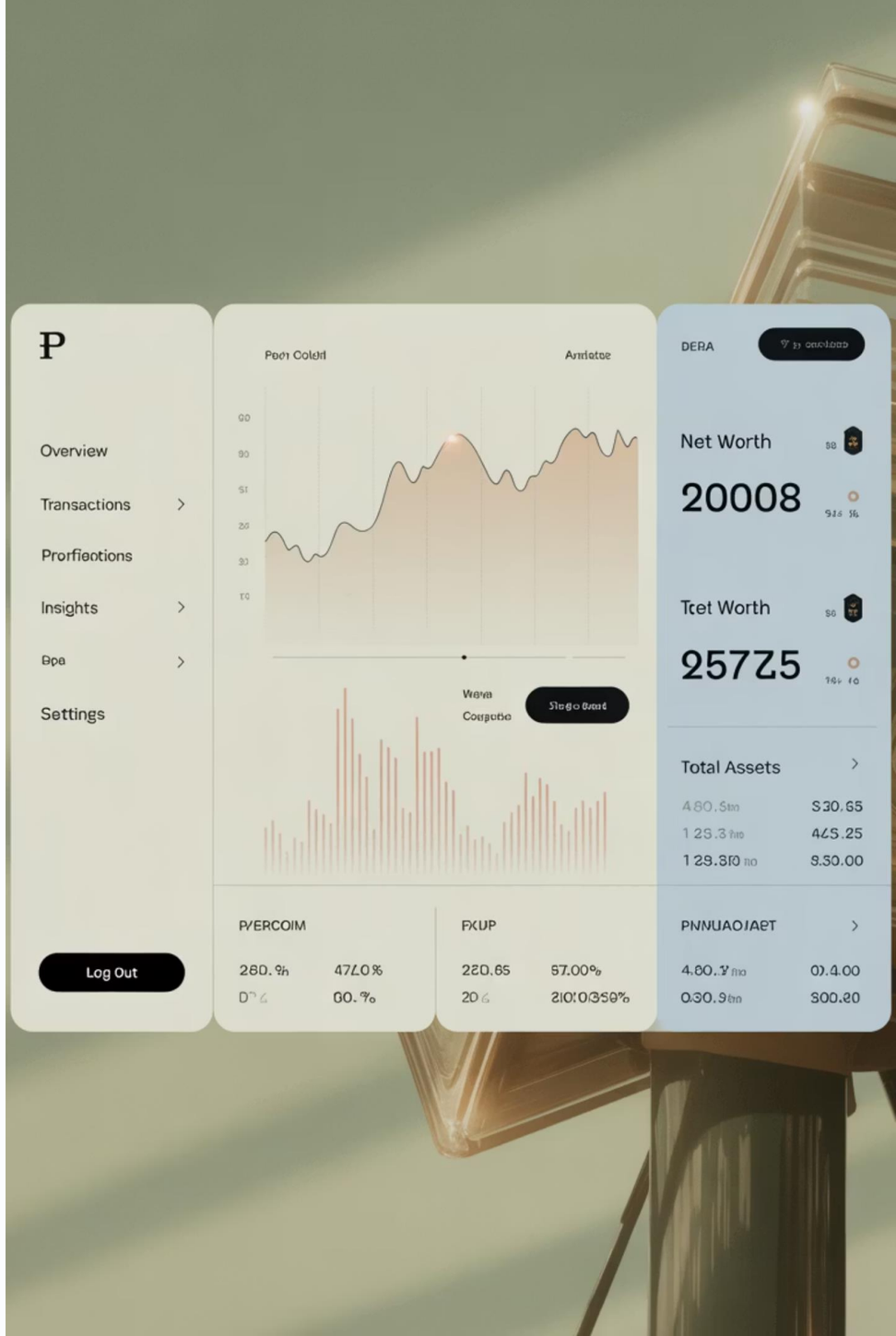
Explainable AI

Advanced models enable fairer credit decisions for credit invisible consumers by providing transparency into their decision-making process. Explainable AI (XAI) helps financial institutions understand the factors contributing to a credit score or a fraud alert, allowing for human oversight, reducing inherent biases in lending practices, and fostering trust with customers.

Autonomous Learning & Action

AI agents continuously self-improve fraud detection and underwriting processes by adapting to new data and evolving threat landscapes. These systems learn from new fraud patterns as they emerge and adjust their models to enhance predictive accuracy, ensuring continuous and proactive protection against financial crimes.

The integration of AI into these core financial operations not only enhances efficiency and security but also paves the way for more inclusive financial ecosystems. As AI continues to evolve, its transformative impact on financial services will only deepen, driving innovation and setting new standards for risk management.

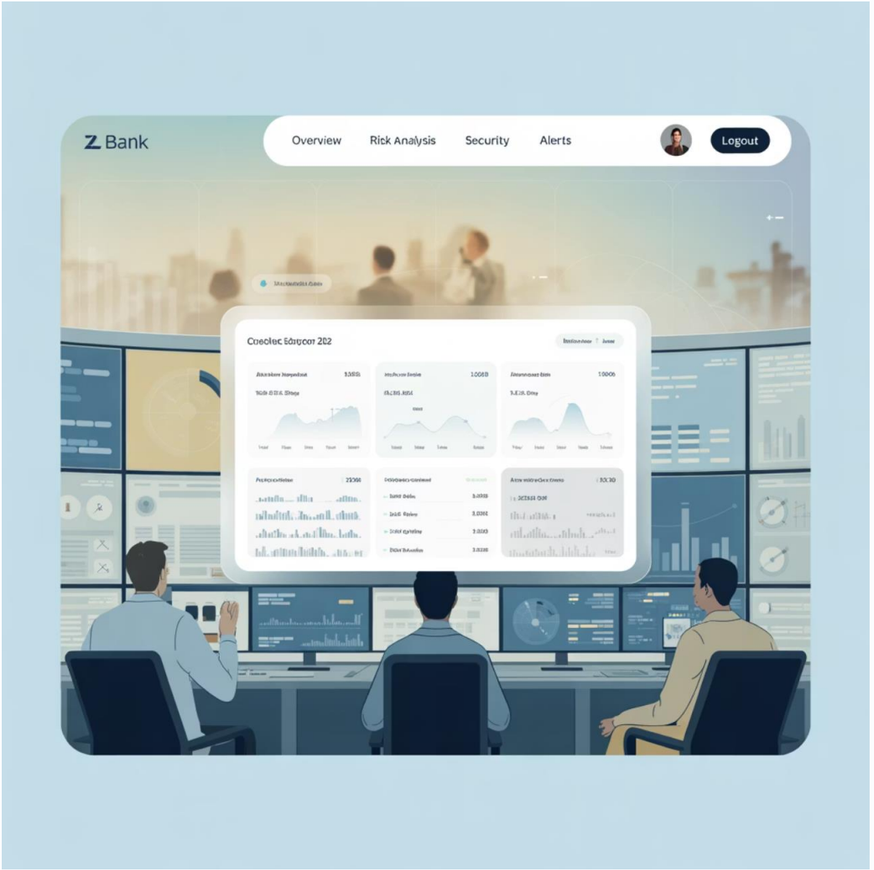


The Dark Side of AI: False Information and Deepfakes

Sophisticated Fraud Techniques

Cybercriminals are leveraging AI to create increasingly sophisticated attack methods that challenge traditional security measures:

- AI-generated deepfakes for identity theft
- Social engineering attacks using voice synthesis
- Behavioral pattern mimicry to bypass detection systems
- Machine learning models trained on legitimate user behavior



Defensive Innovations

Financial institutions are racing to deploy cognitive identity solutions and unforgeable digital signature technologies to combat these emerging threats.

While AI offers unprecedented capabilities for detecting and preventing financial crimes, it simultaneously empowers bad actors with sophisticated tools for perpetrating fraud. This technological arms race requires continuous innovation in defensive measures and careful consideration of AI's dual nature in financial risk management strategies.

AI: The Battleground of Financial Security

Artificial Intelligence presents a paradox in financial services, simultaneously serving as a powerful tool for both sophisticated fraud and robust defense. This creates an ongoing technological arms race between cybercriminals and financial institutions.

1 AI as Risk: Malicious Applications

- **Deepfakes & Voice Synthesis:** Used for highly convincing identity theft and social engineering scams.
- **Automated Attacks:** AI-powered bots execute rapid, adaptive cyber assaults on financial systems.
- **Behavioral Mimicry:** Advanced AI learns legitimate user patterns to bypass traditional detection.

2 AI as Protector: Enhanced Defenses

- **Real-Time Fraud Detection:** AI identifies anomalies and suspicious transactions instantly, preventing losses.
- **Advanced Behavioral Analytics:** Continuously monitors user activity to flag deviations indicative of threats.
- **Predictive Threat Intelligence:** Machine learning models forecast emerging cyber risks for proactive defense.

The rapid evolution of AI demands continuous innovation in defensive measures to stay ahead of increasingly sophisticated threats.

Quantum Computing: The Looming Cryptographic Threat

The Quantum Threat

Quantum computers, with their immense processing power, pose an existential threat to current public-key encryption standards like RSA and ECC, which underpin global financial security and privacy.

- **Data Confidentiality:** Risk of decrypting sensitive customer data and intellectual property.
- **Transaction Integrity:** Potential for compromising payment systems and digital signatures.
- **Blockchain Security:** Vulnerability of distributed ledger technologies to quantum attacks.

The timeline for "quantum supremacy" capable of breaking these ciphers is uncertain but accelerating, necessitating immediate action.

Proactive Mitigation Strategies

Financial institutions must begin preparing now for a post-quantum cryptographic (PQC) era to safeguard assets, maintain trust, and ensure future compliance.

- **Quantum-Resistant Cryptography:** Evaluate and adopt NIST-standardized PQC algorithms for future systems.
- **Cryptographic Agility:** Develop infrastructure capable of easily updating cryptographic primitives as new standards emerge.
- **Post-Quantum Protocols:** Design and implement comprehensive security protocols that are resilient to quantum attacks across all financial operations.
- **Strategic Investment:** Allocate resources for research, talent development, and pilot programs in quantum-safe solutions.

Digital Assets: Reshaping Finance & Risk

The rise of cryptocurrencies, blockchain technology, and Central Bank Digital Currencies (CBDCs) is fundamentally altering the landscape of financial services, presenting both transformative opportunities and significant new risks.

Cryptocurrencies

Volatile assets offer new investment avenues but introduce regulatory uncertainty and market risks for financial institutions.

Blockchain Technology

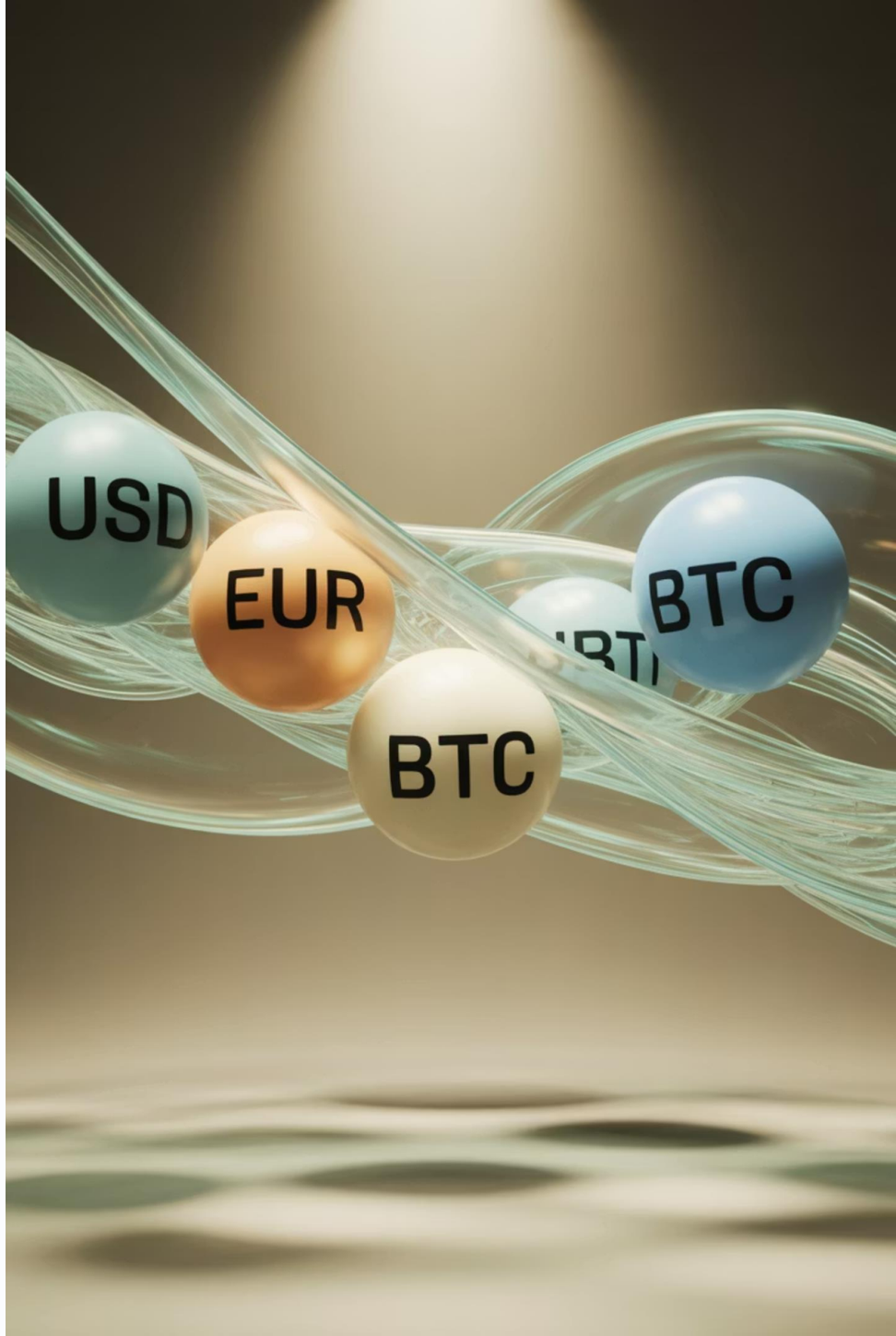
Immutable ledgers enhance security, prevent fraud, and provide transparent transaction trails for improved risk management.

CBDCs

Modernize payment systems, improve financial inclusion, and enable programmable money, while raising new privacy and governance questions.

Regulatory Challenges

Inconsistent global regulations complicate adoption, compliance, and international interoperability of these evolving digital assets.



Agentic AI: Autonomous Agents in Financial Risk

Defining Agentic AI

Agentic AI refers to autonomous artificial intelligence systems capable of acting independently to achieve defined goals. Unlike traditional AI, these agents can perceive their environment, reason about their actions, and execute tasks without constant human intervention, often adapting and learning from new data.

Applications in Banking

Automated Compliance

AI agents continuously monitor transactions and communications against regulatory frameworks, flagging anomalies and ensuring adherence to policies like AML and KYC.

Intelligent Risk Assessment

Agents analyze vast datasets—market trends, customer behavior, geopolitical events—to provide real-time, dynamic risk profiles for portfolios and individual clients.

Autonomous Fraud Investigation

Upon detecting suspicious activity, agents can independently initiate investigations, gather evidence, cross-reference data, and present findings for human review, dramatically accelerating response times.

Predictive Regulatory Reporting

These systems can anticipate future reporting requirements and automatically compile necessary data, ensuring timely and accurate submissions to regulatory bodies.

Benefits for Risk Management

- **24/7 Monitoring:** Continuous oversight of systems and transactions, far beyond human capacity.
- **Faster Response:** Automated threat detection and immediate mitigation actions reduce exposure windows.
- **Reduced Human Error:** Minimizes inconsistencies and mistakes inherent in manual processes.
- **Proactive Threat Detection:** Identifies emerging risks and patterns before they escalate into major incidents.

Implementation Considerations

- **Governance Frameworks:** Establishing clear rules and ethical guidelines for AI agent operations.
- **Human Oversight:** Designing systems with effective human-in-the-loop mechanisms for critical decisions.
- **Regulatory Compliance:** Navigating evolving legal landscapes around AI accountability and data privacy.
- **Inter-Agent Coordination:** Ensuring seamless and secure communication and collaboration between diverse AI agents.

4. RegTech, FinTech, and SupTech

Deployment, Challenges, and Opportunities

The convergence of regulatory technology, financial technology, and supervisory technology is reshaping how financial institutions approach compliance, risk management, and regulatory oversight, creating new opportunities for efficiency while presenting implementation challenges.

RegTech and SupTech: Enhancing Compliance and Supervision

Automated Compliance

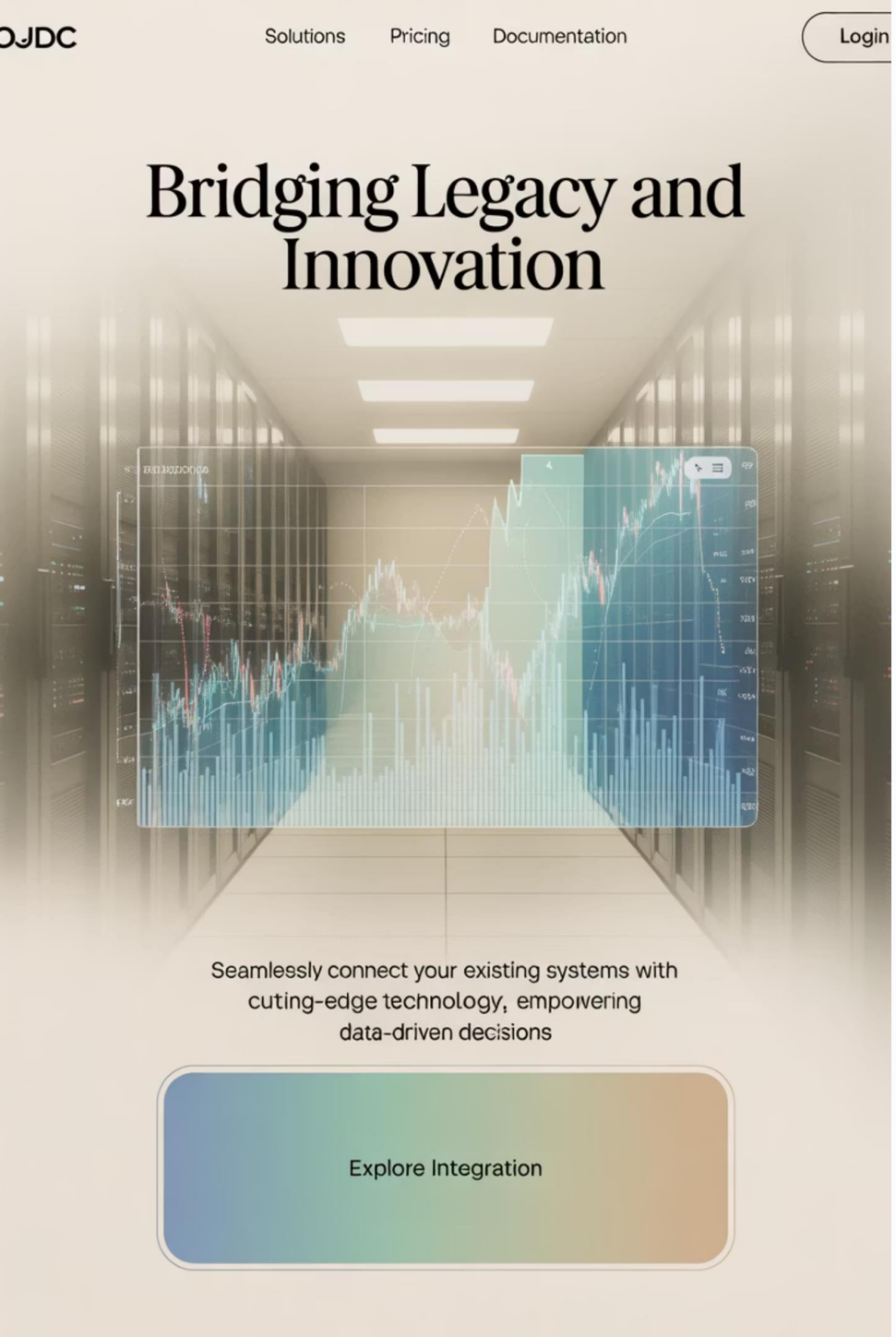
RegTech solutions streamline regulatory reporting and AML compliance processes, significantly reducing manual errors and operational costs while improving accuracy and timeliness.

Real-Time Supervision

SupTech tools provide regulators with unprecedented real-time market surveillance capabilities and advanced risk analytics for proactive oversight.

Collaborative Innovation

Successful implementation requires close collaboration between fintech companies, traditional banks, and regulatory authorities to ensure sustainable innovation.



Challenges in Adoption

Legacy System Integration

Complex integration requirements with existing legacy systems create significant technical hurdles and slow deployment timelines, often requiring extensive customization and testing phases.

Talent Shortage

Critical shortages in specialized talent across AI, cybersecurity, and regulatory expertise domains hamper implementation progress and increase operational risks.

Governance Balance

Organizations struggle to balance innovation speed with robust risk governance requirements, often leading to delayed implementations or inadequate risk controls.

Opportunities Ahead

Unified Risk Platforms

Integrated risk management platforms eliminate data silos and enable holistic risk views across all business lines, improving decision-making and regulatory compliance.

Agentic AI Pilots

Emerging autonomous AI systems promise to revolutionize risk decisioning and operational processes through self-improving algorithms and predictive analytics.

Regulatory Clarity

Increasing regulatory clarity and standardization foster greater market confidence and accelerate fintech scaling opportunities across global markets.

The Future: Connected, Intelligent Risk Management

The future of financial risk management lies in seamlessly integrated systems that leverage artificial intelligence, real-time data analytics, and collaborative technologies to create a comprehensive, proactive approach to identifying, assessing, and mitigating risks across the entire financial ecosystem.

Conclusion: Navigating Innovation with Resilience

Strategic Balance

Success in the digital age requires carefully balancing cutting-edge technological innovation with robust governance frameworks and comprehensive risk management practices.

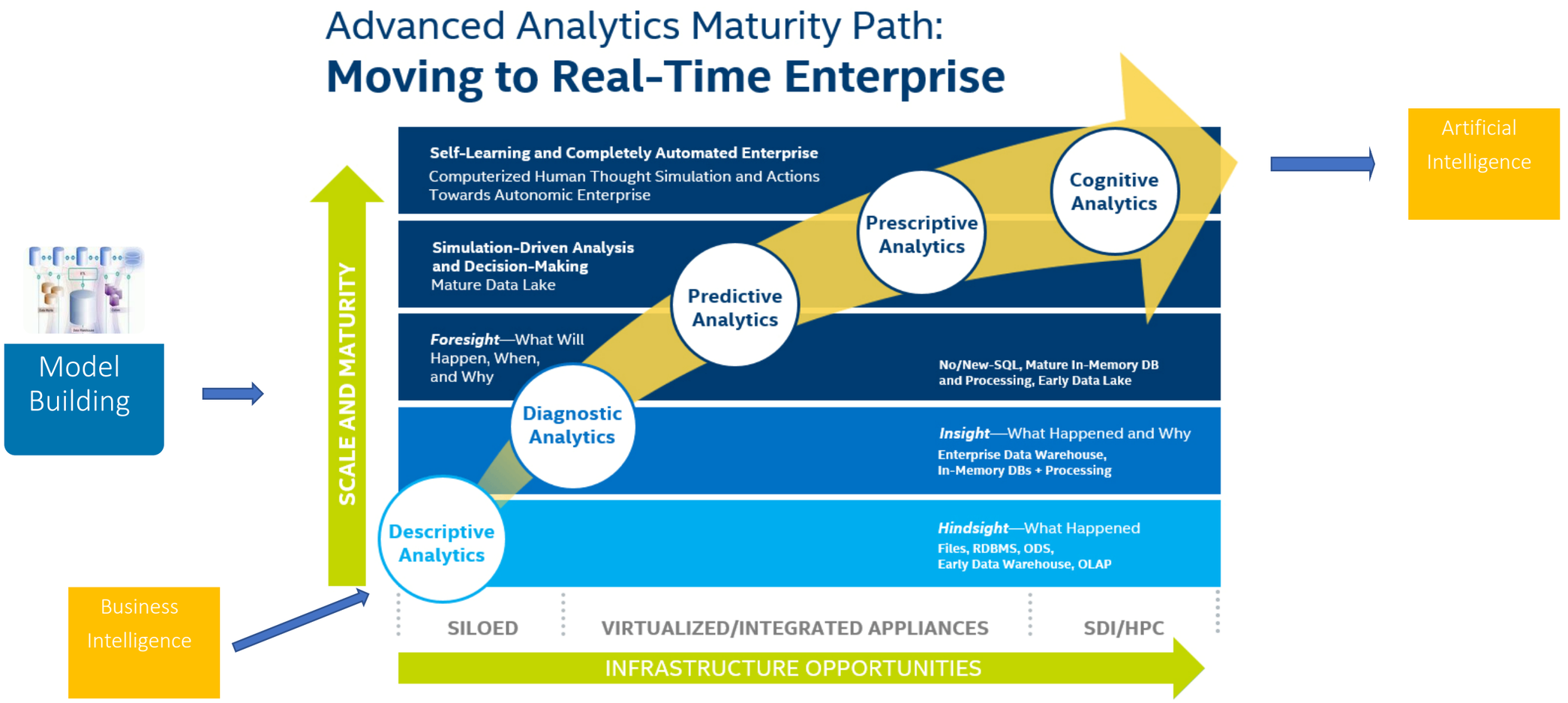
Collaborative Future

Banks, fintechs, and regulators must work together to build a safer, more inclusive financial ecosystem that harnesses technology's benefits while protecting consumers and maintaining system stability.

Responsible Innovation

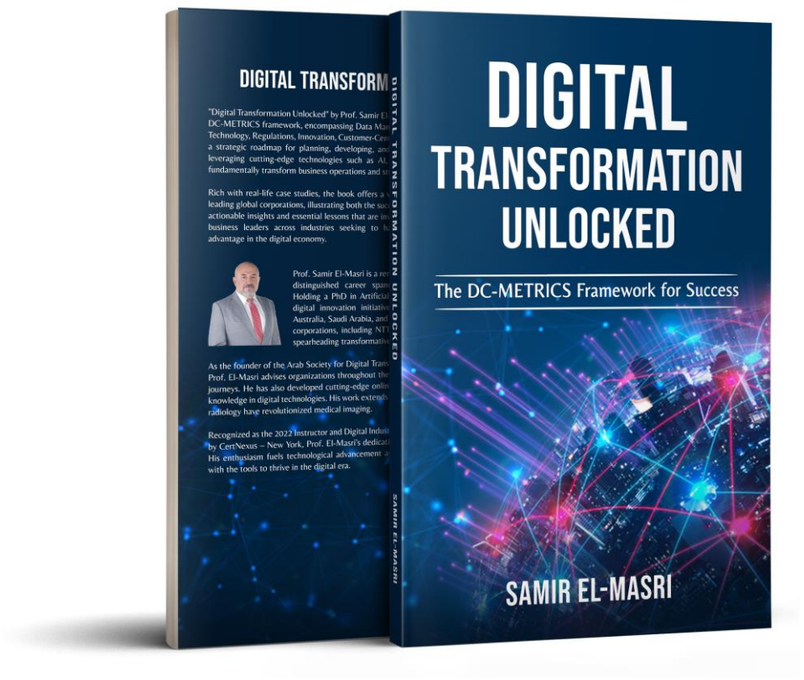
By embracing innovation responsibly and maintaining vigilant risk oversight, the financial services industry can unlock the full potential of digital transformation while ensuring sustainable growth.

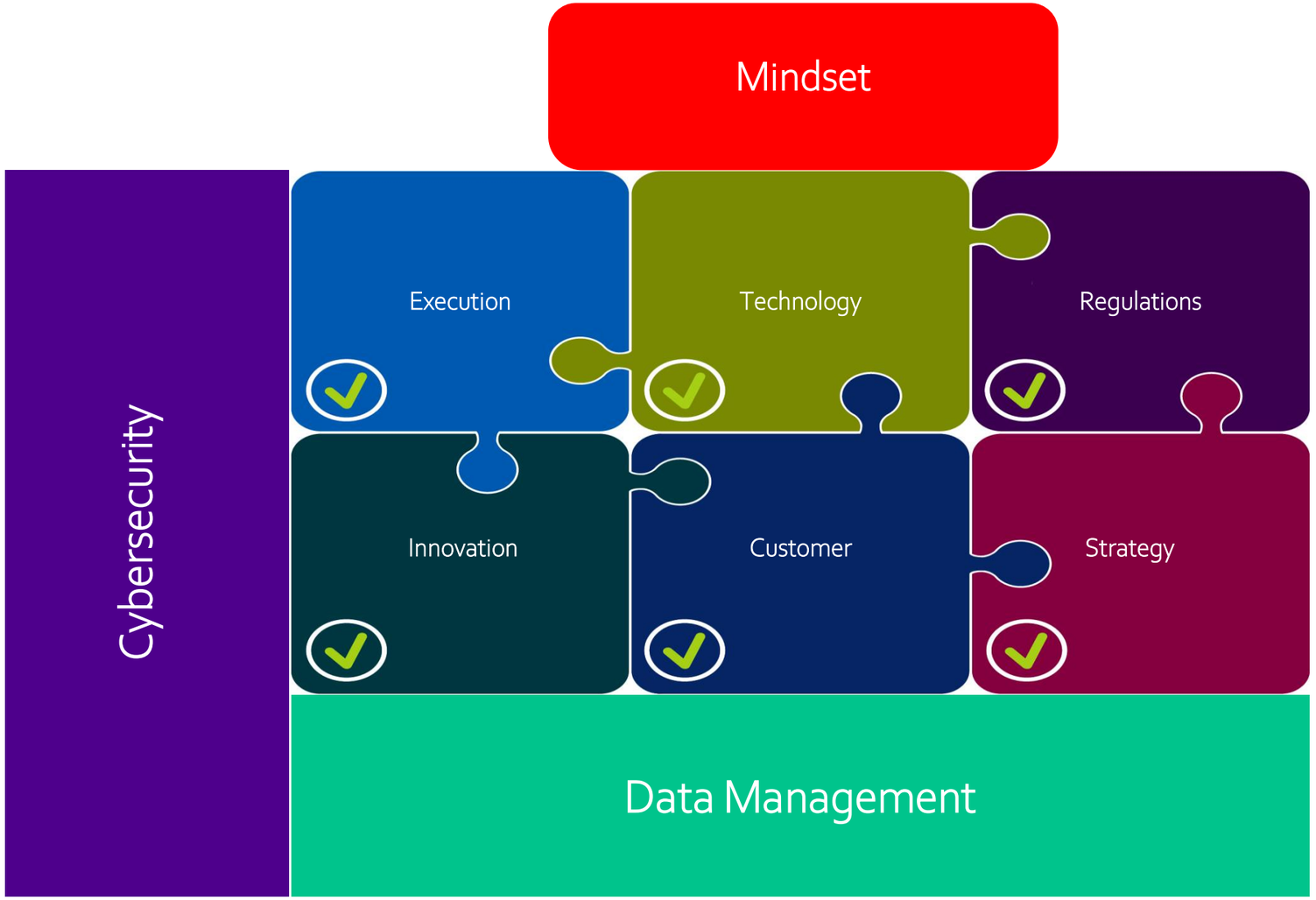
From the basics to maturity



DC-METRICS

Digital Transformation Framework





G20

Digital Cooperation Organization