



Risk Management and Compliance in the Digital Banking Era

Ahmed El Noby
November 2024

“Banking is no longer somewhere you go; it's something you do”

Bank 3.0, Brett King, 2012

“Banking Everywhere, Never at a Bank”

Bank 4.0, Brett King, 2018

- Effective risk management is at the heart of a successful digital bank. It not only protects the bank's assets but also **builds trust with customers.**
- In the digital age, risk management isn't just a necessity; it's a **competitive advantage.**

Digital Transformation Challenges

Rapid adoption of new technologies can outpace the organization's ability to manage associated risks.

Legacy systems may struggle to integrate with modern digital banking solutions, leading to operational inefficiencies.

Employee resistance to change and lack of adequate training can create vulnerabilities.

Digital banking landscape in the Middle East



In **Saudi Arabia**, the Central Bank licensed 3 digital only banks while other applications are in the pipeline as of 2024 .The rise of incumbent banks setting up fully digital arms has been observed

In the **UAE**, both main-land and free zone regulators are licensing digital banks. Wio and Zand received their license from the Central Bank during 2022 and 2023.

Digital banking landscape in the Middle East



The **Qatar** Central Bank is currently looking to license digital banks while developments within regulations like eKYC to regulate online banking continue to be introduced.

The Central Bank of **Egypt** released digital bank and branch licensing regulations in 2023 , and approval to set up a Digital Bank was granted to **onebank**, while other applicants may enter the pipeline in 2025

Digital banking landscape in the Middle East



The Central Bank of **Kuwait** started accepting digital only bank license applications in 2022. While new entrants are in the pipeline, the National Bank of Kuwait (NBK) pioneered digital transformation, through the launch of **Weyay** as Kuwait's first Digital Bank.

The National Bank of **Bahrain** launched its digital banking arm. Bank ABC launched Ila Bank and Singapore Gulf Bank was granted a digital bank license by the Central Bank of Bahrain in 2024

BUSINESS

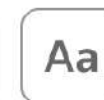
Abrupt shutdown of financial middleman Synapse has frozen thousands of Americans' deposits

In **April 2024**, Synapse Financial Technologies, a fintech company that acted as an intermediary between banks and fintech apps, filed for bankruptcy. This sudden collapse led to the freezing of thousands of accounts for U.S. businesses and consumers, as Synapse's partner banks and fintech clients were unable to access funds. The incident exposed vulnerabilities in the fintech ecosystem, particularly concerning the reliance on third-party service providers.

Fed penalizes Evolve Bank for failing to manage fintech partnership risk

By Hannah Lang and Pete Schroeder

June 17, 2024 11:28 AM GMT+3 · Updated 5 months ago



WASHINGTON, **June 14** (Reuters) - **The Federal Reserve** announced Friday it had ordered Evolve Bancorp Inc to **bolster its risk management programs around fintech partnerships** as well as anti-money laundering laws.

The Fed said in a statement that a 2023 examination of the Arkansas-based bank found **insufficient policies** in place.

It added that the new enforcement action, which did not come with a fine, was independent from bankruptcy proceedings regarding Synapse Financial Technologies, Inc., which the bank had partnered with.

Flagstar Bank Breach Affects 1.5 Million Customers


Bank Discovers Breach 6 Months After Attack; Second Such Incident in 2 Years

Mihir Bagwe ([Twitter](#) MihirBagwe) • June 22, 2022 



In September 2021, Flagstar [agreed](#) to pay \$5.9 million to settle a class action lawsuit filed on behalf of 1.48 million affected consumers. As part of the settlement, the bank pledged "various enhancements" to its third-party vendor risk management program. Victims of the data breach could choose between three years of credit monitoring and identity theft insurance or a one-time cash payout of well below \$1,000. Victims with verifiable financial losses could obtain reimbursements of up to \$10,000.

In January 2021, **Flagstar Bank**, a Michigan-based financial institution, experienced a significant data breach resulting from vulnerabilities in **Accellion's File Transfer Appliance** (FTA). This incident was part of a broader attack that affected multiple organizations utilizing Accellion's services.



FCA fines Starling Bank £29m for failings in their financial crime systems and controls


Press Releases

First published: 02/10/2024

Last updated: 12/11/2024

[See all updates](#)

The FCA has fined Starling Bank Limited £28,959,426 for financial crime failings related to its financial sanctions screening. It also repeatedly breached a requirement not to open accounts for high-risk customers.

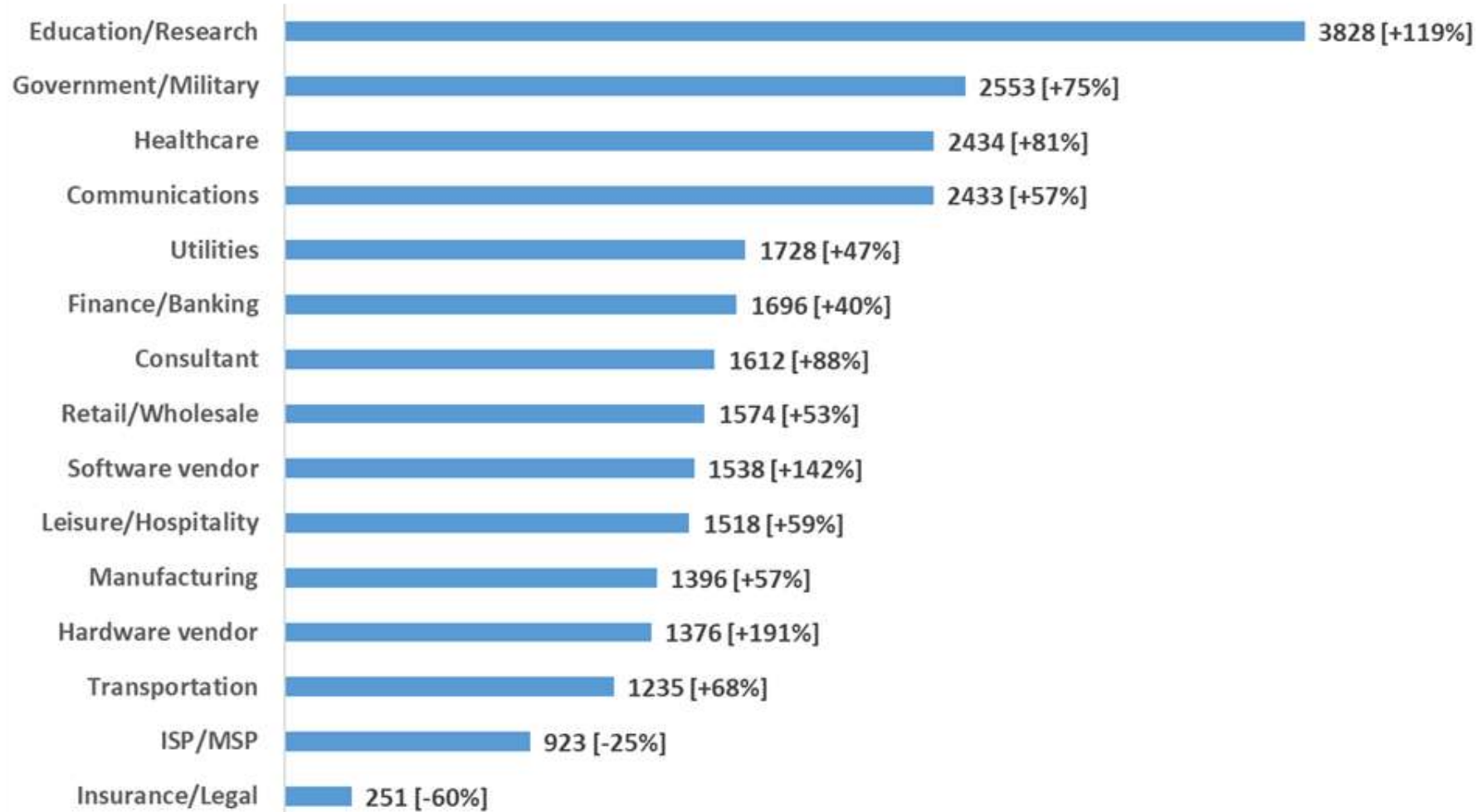


[About](#)[Careers](#)[Investors](#)[Media ▼](#)[Sustainability](#)[Foundation](#)[Research](#)[Login](#)[Media > Listing](#)

DBS apologises for series of digital disruptions; lays out comprehensive roadmap to improve technology resiliency | 简体

In March and May 2023, **DBS Bank**, a leading financial institution in Singapore, experienced **significant service outages** that disrupted its digital banking services, including mobile applications and online banking platforms. **The Monetary Authority of Singapore (MAS)** deemed these disruptions "unacceptable" and imposed additional capital requirements on the bank. These incidents underscore the importance of robust IT infrastructure and risk management in digital banking operations

Global Avg. Weekly Cyber Attacks per Industry (Q3 2024 Compared to Q3 2023)





USD 4.88M

The global average cost of a data breach in 2024—a 10% increase over last year and the highest total ever.

1 in 3

Share of breaches that involved shadow data, showing the proliferation of data is making it harder to track and safeguard.

USD 2.22M

The average cost savings in million for organizations that used security AI and automation extensively in prevention versus those that didn't.



Compliance Challenges in the Digital Era

Data Privacy and Protection

- Laws like GDPR and local data privacy laws require banks to protect customer data rigorously.
- Digital banking demands robust data protection policies and encryption techniques to ensure compliance and safeguard customer information.

Anti-Money Laundering (AML) & Counter-Terrorism Financing (CTF)

- Digital banking can be susceptible to illegal activities such as money laundering. Compliance with AML and CTF regulations is necessary to prevent such activities.
- Utilizing technology like AI in transaction monitoring can help detect and mitigate suspicious activities.

Compliance Challenges in the Digital Era

Cross-Border Compliance

- Cross-border digital transactions introduce complex compliance challenges due to varying regulations across jurisdictions.
- Banks need to ensure compliance with multiple regulatory environments, especially when handling international clients.



Key Drivers for Risk Management

- **Customer Expectations and Trust:** Customers expect secure and seamless digital experiences; breaches or service failures can quickly erode trust.
- **Regulatory Requirements:** As digital banking grows, so does regulatory scrutiny. Compliance with data protection, anti-money laundering, and cybersecurity regulations is essential.
- **Operational Resilience:** Digital banking depends on technology systems that must be robust and resilient to avoid disruptions, which could lead to financial losses and reputational damage.

Operational Risks

- **System Failures and Outages:** Digital banking relies heavily on technology, which can be vulnerable to downtime. System failures disrupt service availability, impacting customer experience and bank operations.
- **Operational Resilience:** Banks need robust strategies to ensure continuity, including backup systems and recovery plans to handle unexpected outages.

Cybersecurity Risks

Data Breaches: Digital banking increases exposure to cyber threats, including data breaches that can compromise customer information and bank security.

Phishing and Identity Theft: Cyber criminals frequently target digital channels through phishing, malware, and identity theft, which can lead to unauthorized transactions and financial losses.

Ransomware and Hacking Attacks: Increasingly sophisticated hacking techniques and ransomware attacks pose significant risks to digital banking platforms, demanding proactive cybersecurity measures and real-time threat detection.

Third-Party Risks

- **External Partnerships:** Collaborations with fintechs and other tech providers introduce risks tied to third-party data management, system compatibility, and operational reliability.
- **Vendor Management:** Effective management of vendors is crucial to ensure compliance and protect customer data when working with third parties.

Reputational Risks

- **Customer Trust:** Any breaches, service failures, or third-party mismanagement can damage customer trust, affecting the bank's image.
- **Social Media Impact:** Negative incidents spread quickly on social media, making proactive reputation management vital.

Risk Management **Strategies** in Digital Banking

Continuous Risk Assessment

- Continuous Risk Assessment is essential in the fast-paced environment of digital banking.
- It involves ongoing identification, monitoring, and evaluation of risks in real time, enabling quicker responses to emerging threats.

Key Points:

1. Real-Time Monitoring and Assessment
2. Dynamic Risk Prioritization
3. Scenario Simulations on the Fly

Risk Management **Strategies** in Digital Banking

Technology-Driven Monitoring

- Technology-driven monitoring leverages advanced tools and systems to enhance risk detection and mitigation.
- In the digital banking era, traditional monitoring methods are insufficient to address the complexities of cyber threats, fraud, and compliance risks.

Key Points:

1. AI and ML for Real-Time Threat Detection.
2. Data Analytics for Fraud Detection.
3. Integrated Monitoring Systems.

Risk Management **Strategies** in Digital Banking

Vendor/3rd Party Risk Management

- Vendor Risk Management is crucial in digital banking, where partnerships with fintechs and third-party service providers are common.
- It ensures that third-party vendors comply with security and operational standards to protect the bank's integrity and customer trust.

Key Points:

1. Establish Third-Party Risk Assessment Protocols
2. Ongoing Monitoring and Auditing:
3. Data Protection and Compliance Assurance
4. Exit Strategies and Continuity Planning

Risk Management **Strategies** in Digital Banking

Regulatory Alignment

- Regulatory alignment ensures that digital banking operations comply with global and local regulations.
- It is critical to maintain customer trust, avoid penalties, and operate securely in a highly regulated environment.

Key Points:

1. Staying Updated with Evolving Regulations
2. Implementing a Governance, Risk, and Compliance (GRC) Framework
3. Cross-Border Compliance Management
4. Training and Awareness

Risk Management **Strategies** in Digital Banking

Crisis Management

- Crisis management is the process of preparing for, responding to, and recovering from unexpected disruptions in digital banking operations.
- With increasing cybersecurity threats and operational risks, effective crisis management ensures continuity and minimizes damage.

Key Points:

1. Developing a Robust Incident Response Plan, BCP, and DRP
2. Real-Time Crisis Communication
3. Post-Crisis Review and Learning

Risk Management **Strategies** in Digital Banking

Customer Education

- Educating customers about risks and safeguards in digital banking is crucial for mitigating threats such as phishing, identity theft, and unauthorized access. Empowered and informed customers act as the first line of defense against cybersecurity risks.

Key Points:

1. Awareness Programs on Cybersecurity Risks
2. Transparent Communication on Data Protection
3. Encouraging Safe Digital Practices
4. Accessible Educational Resources

Risk Management Frameworks in Digital Banking

COSO ERM:

- Provides a structured approach to identify, assess, and manage risks within digital banking environments.

ISO 31000:

- International standard offering principles and guidelines for risk management, focusing on integration into organizational processes.

NIST Cybersecurity Framework:

- Tailored for managing cybersecurity risks in financial institutions, emphasizing identification, protection, and response.

NIST AI Risk Management Framework:

- Focuses on governing AI systems to ensure they are trustworthy, secure, and resilient.
- Emphasizes the pillars of accuracy, fairness, transparency, and privacy.

ISO/IEC TR 24028:

- Provides guidelines for ensuring robust AI system governance, including security, reliability, and ethical considerations.

Internal Audit Considerations

1. Risk Identification and Assessment

- Use comprehensive tools to identify potential risks in digital banking, including risk assessment frameworks and regular monitoring.
- Regular risk assessments help in early detection and mitigation.

2. Digital Audit Tools

- Leverage data analytics, artificial intelligence, and machine learning for effective auditing of digital banking processes.
- Digital audit tools enhance risk identification by analyzing large data sets for unusual patterns.

3. Continuous Auditing

- Adopting a continuous audit approach provides timely insights and allows for quicker responses to emerging risks.
- Continuous auditing is especially effective in the dynamic environment of digital banking.



Questions

?

?

Answers

?