S|3 SPECIALIZED SECURITY SERVICES

SAFEGUARDING TRUST

The Crucial Role of Compliance & Technological Evolution for Financial Institutions

THE TECHNOLOGY COMPLIANCE LANDSCAPE FOR FINANCIAL INSTITUTIONS

Regulation and compliance are not new topics within the Financial Services industry. Companies in this sector have been facing scrutiny and regulation for years. However, the regulatory landscape is continuously evolving and expanding due to the introduction of new technology and increasing demands on companies to deliver more services rapidly and in a more convenient manner.

Companies operating in today's high-pressure economy are searching for ways to "do more with less," while maintaining the trust of their customers. This has led to accelerated growth in technology, rapid evolution of AI and quantum computing, and an expansion of customer offerings and tools beyond traditional banking services.

With all of this change, the big questions financial institutions (FIs) are facing include:

- What top-of-mind technology risks should FIs be assessing?
- What are the compliance implications and what will regulators be focusing on in the near future?
- How can financial institutions prepare to meet these evolving requirements and challenges?

Before diving into FI regulatory and compliance practices, let us consider some of the current technology trends for FIs and how those can translate into increased risks.

TOP TECHNOLOGY TRENDS FOR FINANCIAL INSTITUTIONS

Rapid Evolution of AI is reshaping the landscape for financial institutions, with automation playing a pivotal role in supporting Control Assessments (NIST IR 8001). Deep learning algorithms are increasingly employed to enhance decision-making processes, ranging from compliance and underwriting to investment management.

The integration of chatbots is revolutionizing customer service and overall experiences for financial institution clients. Leveraging AI, these chatbots are becoming indispensable tools for providing efficient and personalized services that elevate customer satisfaction and engagement.

Quantum Computing is emerging as a transformative force within the financial sector, particularly in investment management. Firms are leveraging quantum computing capabilities to drive opportunities in portfolio optimization and calculate complex derivatives, positioning themselves strategically to stay ahead of the competition.[1] Distributed Ledger Technology (DLT) is gaining prominence, with applications ranging from cryptoasset custody to tokenized real-world assets and liabilities. Financial institutions are exploring the potential of DLT to streamline processes, enhance security and unlock new avenues for innovation.[2]

Increased Contactless Payment Devices reflect the ongoing digital transformation in the financial sector. As banks expand their digital and electronic product offerings, services and capabilities, the adoption of contactless payment devices is becoming more widespread, offering customers convenient and secure transaction options.

TOP TECHNOLOGY RISKS FOR FINANCIAL INSTITUTIONS

Virtual Currency Investment Scams

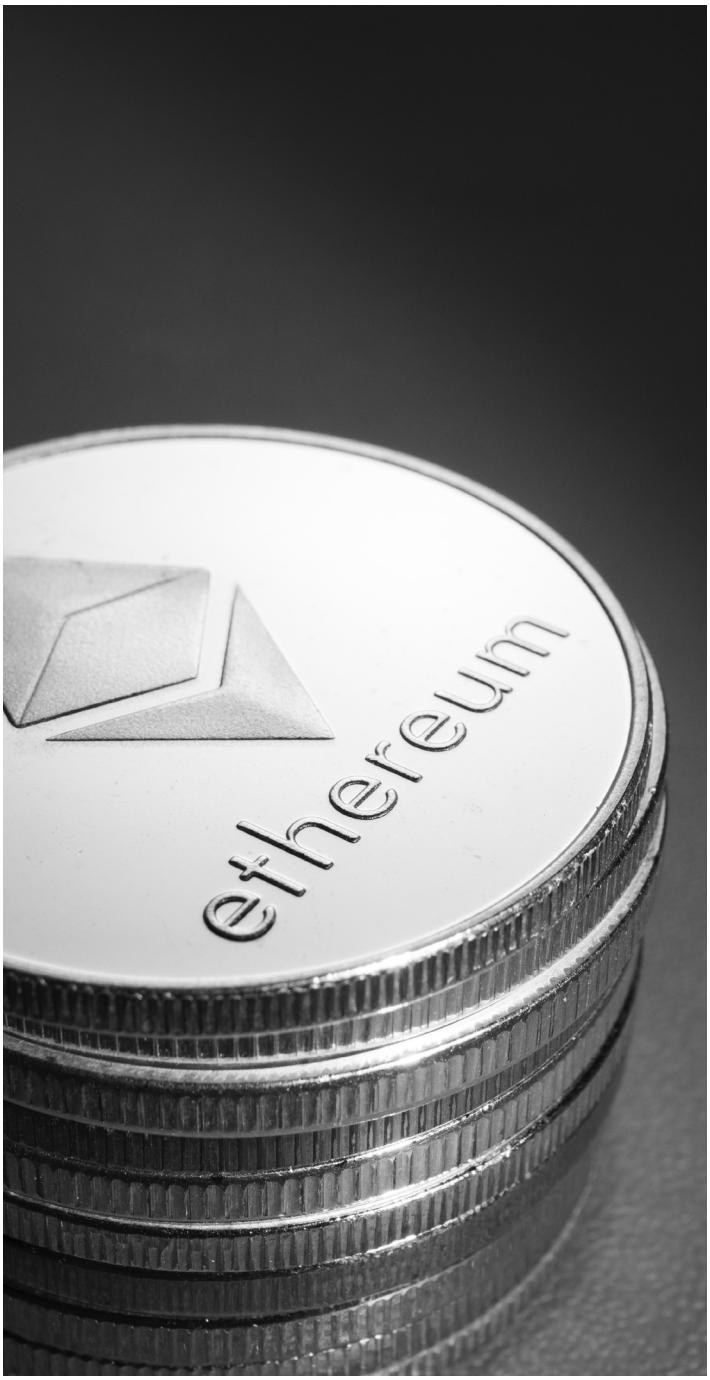
Financial institutions face a growing threat from virtual currency investment scams, with the "Pig Butchering" scheme gaining prevalence in 2023.[3]

DDoS Attacks

Financial institutions remain vulnerable to Distributed Denial of Service (DDoS) attacks, as cyberthreats persistently target weak or poorly configured authentication controls. The ongoing threat of DDoS attacks necessitates continuously enhancing cybersecurity measures to protect against potential disruptions.[4]

Maintaining Legacy Technology Architectures

The challenge of maintaining legacy technology architectures while meeting the escalating demands of digitalization and balancing technology debt presents a notable risk for financial institutions. Striking a balance between technological modernization and the need for robust cybersecurity measures is imperative to navigating the evolving landscape without compromising system integrity or data security.



IT/CYBERSECURITY FOCUS AREAS OF FINANCIAL INSTITUTION REGULATORS & EXAMINERS

As highlighted in the OCC News Release 2023-109: Bank Supervision Operating Plan for Fiscal Year 2024[5] these are the key areas of heightened focus for examiners:

Incident Response

Financial institution regulators and examiners are placing a heightened focus on evaluating incident response processes, ensuring compliance with regulatory reporting requirements and assessing banks' capabilities in handling incidents – including those involving ransom or other extortion demands.

Third Party Risk Management

Emphasizing the critical nature of third-party risk management, regulators urge examiners to assess the effectiveness of banks' approaches, specifically validating third-party controls and data protections such as access management, network management, data management and, potentially, how FIs will manage service providers who are utilizing their own third-party providers and/or AI.

BSA/AML Controls and Evaluation

In response to the evolving landscape of payment methods and accessibility, regulators stress the continual evaluation of BSA/AML controls. This includes adapting to new or changing risk profiles, such as launching instant payments via FedNow that ensure banks continuously assess their BSA/AML risks and corresponding controls.

Asset Inventory/End-of-Life Risk Management

Acknowledging the significance of end-of-life risk management, regulators direct examiners to evaluate banks' processes for inventorying IT assets and determining asset life cycles. This includes considerations such as the expected end-of-life for Microsoft Windows 10 in 2025.

Cyber Intelligence Gathering and Analysis

Regulators highlight the importance of evaluating cyber intelligence gathering and analysis. This encompasses a comprehensive assessment of threat, vulnerability detection and remediation, as well as robust software patch management practices.

Organization-Wide Change Management

Recognizing the growing customer demand for technology, regulators advocate for comprehensive organization-wide change management. This involves implementing secure Software Development Life Cycle (SDLC) and DevOps controls, ensuring systems and applications tied to service offerings are designed, developed, deployed and implemented securely. Additionally, regulators underscore the need to evaluate changes resulting from mergers and acquisitions, system conversions and/or regulatory

requirements, and implementing new, modified or expanded products and services – including technological innovations.

Acceptable Use of AI

As stated in the OCC's Semiannual Risk Perspective Fall 2023 report: "Although existing guidance may not expressly address AI use, the supervision risk management principles contained in OCC issuances provide a framework for banks that implement AI to operate in a safe, sound and fair manner. It is important for banks to identify, measure, monitor and control risks arising from AI use as they would for the use of any other technology."[4]

Acceptable Use policies for AI are essential for FIs as usage continues to expand, enabling employees to make good decisions while adhering to pertinent regulations. Tenets of a sound policy include confidentiality, responsibility, access, monitoring, accuracy and attribute output.[6] The use of AI should also reflect the culture and ethics of the company. Use should comply with applicable laws, rules, and regulations, including privacy requirements. In addition to acceptable use, incident response should address data incidents related to AI, and employee acknowledgment/training should also address AI.

PROPEL YOUR BUSINESS FORWARD

The regulatory compliance landscape for financial institutions demands a strategic and proactive approach in the face of evolving technological challenges and opportunities. As emphasized in the OCC's semiannual Risk Perspective for Fall 2023, operational resilience is critical to mitigating disruptions arising from various hazards, including cyberthreats and technology outages.

Compliance can be expensive, but non-compliance is far more costly. As FIs of all types and sizes search for ways to stay profitable, reputation is a key factor that can increase or decrease customer activity and satisfaction. Prioritizing and directing efforts toward robust data privacy protection aligns with compliance requirements and establishes a solid foundation for maintaining integrity and trust.

Financial institutions in all categories including banks, credit unions, insurance providers and commercial lenders must remain continuously aware of emerging technology and the associated risks in order to implement appropriate controls that mitigate such risks.

By embracing these key insights and adopting best practices, financial institutions can navigate the complex regulatory environment, foster operational resilience and secure the trust of their customers in an increasingly interconnected and digital world.

BE READY WITH COMPREHENSIVE CYBERSECURITY AND COMPLIANCE SUPPORT FROM S3 SECURITY

No matter where you are on your cybersecurity compliance journey, S3 Security is your dedicated partner. With a proven record of accomplishments in guiding financial institutions through complex regulatory landscapes, we are positioned to help you in navigate the dynamic challenges of an evolving technology and a shifting regulatory landscape.

Recognizing the unique challenges financial institutions face today, we understand that compliance is not just an obligation but a pathway to professional peace of mind. Compliance with FFIEC, GLBA, SOX and other existing regulatory requirements are mandated and critical for any financial institution.

S3 Security is experienced in partnering with financial institutions as a trusted advisor to assist with any existing regulatory compliance issues. However, it is becoming increasingly clear that there are a wide range of new and innovative technologies and associated cybersecurity risks facing the financial industry.

This is causing FI's to seek out partners who are not only experienced in both assisting with "blocking and tackling" regulatory requirements from the FFIEC, OCC, etc., but also possess the knowledge, skills and expertise to advise them on the latest technology and enable them to reap all the benefits while avoiding the risks.

Reach out to us today. Let our experts will walk you through the intricacies of the evolving regulatory landscape and offer insights into the latest requirements, updates to controls, testing procedures and reporting. Discover how embracing these best practices can ensure compliance, foster operational resilience and increase the trust of your customers.

RESOURCES:

1. Deloitte Podcast: Financial services industry faces tradeoffs in 2024 https://www2.deloitte.com/us/en/insights/multimedia/podcasts/financial-services-industry-trends-podcast.html
2. BCG Presents - Impact of Distributed Ledger Technology in Global Capital Markets https://www.gfma.org/wp-content/uploads/2023/05/impact-of-dlt-on-global-capital-markets-full-report.pdf
3. FinCEN Issues Alert on Prevalent Virtual Currency Investment Scam Commonly Known as “Pig Butchering - https://www.fincen.gov/news/news-releases/fincen-issues-alert-prevalent-virtual-currency-investment-scam-commonly-known
4. OCC Semiannual Risk Perspective Fall 2023 - https://www.occ.treas.gov/publications-and-resources/publications/semiannual-risk-perspective/files/semiannual-risk-perspective-fall-2023.html
5. OCC Bank Supervision Operating Plan for Fiscal Year 2024 - https://www.occ.gov/news-issuances/news-releases/2023/nr-occ-2023-109.html
6. FS-ISAC Framework of an Acceptable Use Policy for External Generative AI - https://www.fsisac.com/hubfs/Knowledge/FrameworkOfAnAcceptableUsePolicyForExternalGenerativeAI.pdf?hsLang=en