Beyond Pilots and Sandboxes

Regulatory Innovation through SupTech Case Studies and Leading Practices

Nick Cook • Saket Narayan

June 2025

TABLE OF CONTENTS

INTRODUCTION

The rise of digital financial services has significantly expanded financial inclusion globally, bringing millions of previously unserved individuals and businesses into the formal economy. These services have unlocked new opportunities for innovation, efficiency, and economic growth, enabling faster payments, more accessible credit, and cost-effective financial products tailored to diverse needs and customer preferences. In parallel, financial regulators and central banks globally need to innovate beyond traditional approaches to oversight and regulation to ensure adequate protection for consumers, assure the safety and soundness of the financial sector and mitigate the risk of financial crime.

However, this transformation also introduces significant risks. The rapid adoption of digital platforms has heightened exposure to fraud and scams, market instability, and systemic vulnerabilities. Regulators must contend with complex, cross-border financial systems, evolving consumer behaviors, and sophisticated criminality—all while maintaining public trust and financial stability. Regulators today face increasing challenges in performing their licensing, supervising, and oversight duties efficiently at an ever greater scale in the financial sector.

Regulators must contend with complex, cross-border financial systems, evolving consumer behaviors, and sophisticated criminality—all while maintaining public trust and financial stability.

Supervisory Technology (SupTech)[1], offers a way forward. Using modern technologies regulators can streamline regulatory processes, enhance decision-making, and scale oversight capabilities to address the growing complexity of globally connected economies. Global focus and investment in SupTech has grown steadily, as highlighted by various surveys and reports[2]. However, many regulators face challenges in identifying where to begin investing when resourcing is constrained, and in transitioning from pilots to full-scale implementation and adoption.

This paper explores how regulators can harness SupTech to combine innovation with resilience, efficiency with integrity, and modernization with public trust. Drawing on case studies and proof-of-concept projects it offers practical guidance to build capabilities that address today's regulatory challenges. By fostering a culture of experimentation, collaboration, and data-driven decision-making, regulators can seize the opportunities of digital transformation while mitigating its risks.

[1] *Singapore FinTech Journey 2.0*. This 2017 speech by MAS' Managing Director Menon was the first recorded use of the term 'suptech'. "*It is not only the financial industry that needs FinTech, but regulators as well. MAS has embarked on its own FinTech journey to make our supervision more effective and the compliance burden we impose less painful. We call it Supervisory Technology, or SupTech for short.*" https://www.bis.org/review/r171115a.pdf

[2] https://www.bis.org/fsi/publ/insights58.pdf;
https://lab.ccaf.io/wp-content/uploads/2024/12/Cambridge-SupTech-Lab-State-of-SupTech-2024-Exec-Summary-1.pdf

BEST PRACTICES FOR SUPTECH IMPLEMENTATION

Effectively deploying SupTech requires a strategic balance of creativity and rigor. These best practices guide regulators in integrating advanced technologies into their supervisory functions:

Start with a Clear Strategic Vision:

A purpose-driven vision ensures that technology initiatives align with regulatory objectives. Priorities may include addressing known blind spots in the regulatory oversight of specific product and asset classes; streamlining costly and inefficient manual processes; or focusing on dynamic products and markets where regulatory decision-making currently relies only on historical or backward-looking perspectives. By setting measurable goals and prioritizing resources, regulators can avoid adopting technology for its own sake and maintain focus on long-term outcomes.

Position Data as a Core Asset:

Data should be treated as a strategic asset that drives decision-making and enhances agility. This requires development of robust data governance frameworks and analytics capabilities, supported by investments in modern cloud-based data platforms and talent. A dual approach—recruiting new specialists and upskilling existing staff—ensures that teams have both technical and regulatory expertise.

Data should be treated as a strategic asset that drives decision-making and enhances agility.

Foster Collaboration and Knowledge Sharing:

Collaboration, both internally and externally, is key to addressing complex regulatory challenges. Internally, cross-functional teams and shared lessons ensure that innovation scales across the organization. Externally, participation in regulatory sandboxes, TechSprints[3], industry working groups, public-private forums[4], and other international initiatives provide opportunities to learn from diverse stakeholders and stay ahead of emerging trends. Leaders should incentivize collaboration by recognizing and rewarding contributions.

Cultivate Talent and the Right Mindset:

Effective SupTech deployment relies on a workforce equipped with the right skills and mindset. Leaders must foster a culture of experimentation, encouraging intellectual curiosity and calculated risk-taking. Upskilling programs help staff adapt to new technologies, while leadership modeling sets the tone for innovation.

Adopt an Agile, Iterative Approach:

Regulators should adopt a product-focused mindset when developing SupTech solutions, treating regulations and supervisory tools as iterative products. Multidisciplinary teams—spanning policy, supervision, technology, data science, and user-centric design—can be organized around specific regulatory outcomes, delivering repeatable value to both regulators and regulated entities. These teams should leverage agile methodologies to experiment, gather real-world feedback, and continuously refine solutions. By understanding the expectations, processes, and journeys of regulated entities and colleagues, this approach ensures SupTech tools evolve to improve user experience and utility.

---

[3] TechSprints are collaborative, time-bound innovation events tackling regulatory or financial challenges using technology and cross-sector expertise. See for example - https://regulationinnovation.org/techsprints/; https://apixplatform.com/case-studies; and https://www.fca.org.uk/firms/innovation/techsprints.

[4] For example, the Monetary Authority of Singapore's Financial Sector Cloud Resilience Forum www.mas.gov.sg/news/media-releases/2023/mas-establishes-financial-sector-cloud-resilience-forum, or the US TreasuryCloud Executive Steering Group (a public-private partnership, consisting of US banking agency heads and sector executives) - https://home.treasury.gov/about/offices/domestic-finance/financial-institutions/cloud-executive-steering-group

Balance Innovation with Security and Resilience:

Innovation must be twinned with robust security and resilience. As systems and processes are digitized, leaders must implement strong cybersecurity protocols and risk management frameworks to safeguard operations[5]. Emphasis should be given to agency security and operational resilience, including use of and support for secure reading rooms. Supervisory teams should be trained on and held to a high bar for security. All confidential information must be handled exclusively through authorized digital channels within secure environments, strictly prohibiting physical copies, off-premise transfers, or unauthorized digital captures including mobile device screenshots in reading rooms.

Cloud adoption remains key to building contemporary supervisory capabilities:

Cloud adoption empowers supervisory authorities to leverage cutting-edge technologies such as artificial intelligence (AI) and machine learning (ML), enabling real-time data analytics, enhanced risk monitoring, and automated compliance processes at scale. By utilizing cloud services, supervisors can rapidly deploy new supervisory tools, adapt to emerging financial risks, and efficiently process vast amounts of regulatory data while maintaining the highest standards of security and operational resilience. Furthermore, cloud technology can provide the agility and cost-effectiveness needed to keep pace with the rapidly evolving financial sector, allowing supervisors to effectively oversee increasingly digital financial services and implement sophisticated regtech solutions without the burden of managing complex physical infrastructure. To achieve enhanced resilience and operational excellence in cloud-based supervisory systems, supervisory authorities must comprehend and implement the shared responsibility model with their Cloud Service Provider (CSP)[6], clearly delineating security and operational accountabilities between both parties. When selecting cloud services, supervisory authorities must carefully evaluate their responsibilities, which vary depending on the specific services chosen, their integration into existing IT environments, and applicable regulatory requirements. This differentiation of responsibility, commonly referred to as Security "of" the Cloud versus Security "in" the Cloud, provides the necessary flexibility and control for effective deployment while ensuring clear accountability for both parties in maintaining a secure and compliant infrastructure. Organizations should ensure cutting-edge solutions do not compromise security or resilience.

[5] The Cyber Risk Institute's Profile approach is garnering global uptake as it marries global standards (ISO, NIST, IOSCO) to the body of global security and operational resilience regulations for a more globally aligned approach to self-assessments, risk management, and oversight of the use of IT and cloud services. https://cyberriskinstitute.org/

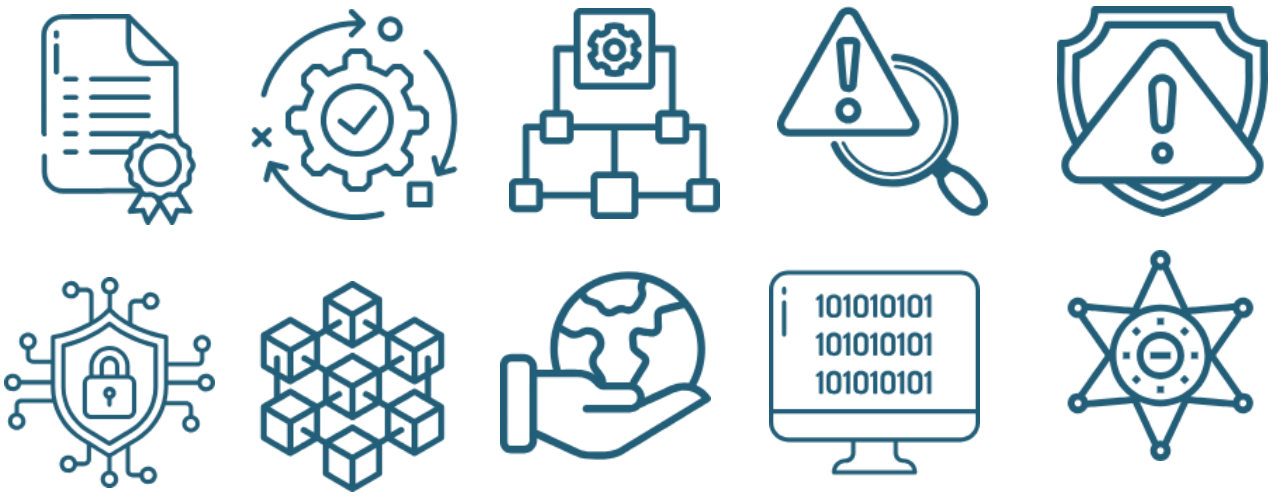
[6] See, for example https://aws.amazon.com/compliance/shared-responsibility-model/

THE CORE CAPABILITIES

This paper identifies core capabilities required for regulators to effectively supervise, monitor, and manage risks in the financial services sector. They include areas where regulatory interest in SupTech is pronounced and where progress has been uneven to date, highlighting opportunities for knowledge-sharing and collaboration.

- **Licensing and Case Management:** Streamlining processes for approving and monitoring new financial firms to promote competition and financial inclusion.
- **Business Model Analysis:** Evaluating how regulated entities generate revenue and sustain profitability.
- **Assessment of Governance Practices:** Ensuring regulated entities maintain effective decision-making, risk management, and compliance frameworks.
- **Financial and Microprudential Risk Assessment:** Evaluating individual regulated entities' stability and resilience.
- **Macroprudential and Systemic Risk Assessment:** Monitoring systemic risks that could impact financial stability.
- **Cyber Risk Detection and Monitoring:** Addressing the increasing threat of cyberattacks and digital vulnerabilities.
- **Digital Asset Monitoring and Oversight:** Supervising blockchain-based financial instruments and decentralized finance.
- **Environmental, Social, and Governance Reporting:** Enhancing transparency and accountability in sustainability practices.
- **Regulatory Reporting and Data Collection:** Modernizing data submission and analysis for efficiency and compliance.
- **Investigation and Enforcement of Regulatory Violations:** Using advanced tools to detect, investigate, and address regulatory violations efficiently.

Each capability is considered in turn, outlining challenges, specific technological solutions, and real-world case studies. The aim is to inspire actionable approaches that regulators can adapt to their unique contexts.



Licensing and Case Management

The licensing and case management process is foundational to regulatory oversight, ensuring that both new financial firms and existing regulated entities operate within a sound legal framework. As the financial ecosystem grows more diverse and digital, regulators face increasing demands to assess, approve, and monitor applicants swiftly and thoroughly. Efficiency, consistency, and accuracy in licensing are critical to maintaining market integrity, fostering competition, and supporting financial inclusion.

Traditional licensing processes, often manual and time-consuming, create bottlenecks and burdens for regulators and applicants alike. The rise of fintechs, digital banks, and innovative financial entities further complicates this landscape, while regulatory arbitrage and the cross-border nature of many institutions heightens risks. Addressing these challenges requires a technology-driven approach to streamline operations and improve decision-making.

SupTech tools enable regulators to modernize licensing by automating repetitive tasks, enhancing data analysis, and integrating timely insights from varied sources. These solutions reduce manual burdens, improve accuracy, and provide regulators with the tools to focus on high-value activities. In conjunction with test-and-learn approaches such as regulatory sandboxes, regulators can refine and right-size their approach to licensing and leverage technology to ensure risks are properly identified, monitored and managed.

Smart Document Processing

Optical character recognition (OCR), natural language processing (NLP), and generative AI capabilities such as large language models (LLMs) can transform how regulators review and analyze documents such as business plans, financial statements, and compliance records. These systems can extract, categorize, and evaluate critical information, flag inconsistencies, and reduce the time required for manual review - indeed such systems can operate at scale and workloads far in excess of human labor.

The European Central Bank's (ECB) Heimdall tool[7] uses OCR, automated translation, and NLP to assist with fit-and-proper assessments by European banking supervisors. By reducing manual workloads and the potential for human error, Heimdall has enhanced the ECB's ability to handle large volumes of unstructured data efficiently.

LLMs fine-tuned for regulatory contexts offer the ability to synthesize complex documents, identify gaps or risks, and suggest plausible corrections. These models understand nuanced legal and compliance terminology, improving the quality and depth of document review processes. Regulators are increasingly exploring development of such models (both individually and in collaboration with the private sector[8] and peer regulators) to handle the unique demands of licensing and supervision.

The Australian Securities and Investments Commission (ASIC)[9], Australian Prudential Regulation Authority (APRA), and the Reserve Bank of Australia (RBA) recently worked alongside AWS to build a generative AI proof of concept (PoC) solution to compare, query and summarize documents. Prioritizing responsible AI principles, the PoC achieved promising results, including as much as 93 percent confidence in some model outputs using publicly available documents. The experiment has been shared with dozens of other regulators and provides a glimpse into the future of regulatory practices and financial oversight.

---

[7] https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/ecb-supervisory-boost-gen-ai/

[8] Private sector development of fine-tuned LLMs, such as those developed by Bloomberg and AWS provide further inspiration and evidence of the value of such approaches - https://aws.amazon.com/blogs/industries/the-next-frontier-generative-ai-for-financial-services/ and https://aws.amazon.com/blogs/machine-learning/domain-adaptation-fine-tuning-of-foundation-models-in-amazon-sagemaker-jumpstart-on-financial-data/

[9] https://pages.awscloud.com/ps-symposium-canberra-on-demand.html

AI-Driven Risk Profiling

Machine learning models analyze historical and contextual data to generate risk scores for new applicants. By focusing on high-risk entities, regulators can prioritize their resources where they are most needed.

Automated Compliance Verification

Automated tools help ensure new institutions meet regulatory standards, such as Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements, by linking licensing systems with compliance databases. The Bank of Portugal[10] deployed NLP algorithms to automatically validate compliance with pre-defined rules for credit agreements. This pilot significantly reduced manual efforts, verifying up to 20% of compliance rules automatically. Similar approaches could be extended to licensing evaluations, supporting analysis of adherence to key regulatory requirements and freeing up scarce human resources.

Graph Analytics and AI-Driven Risk Scoring for Relationship Mapping

Graph-based tools and AI-driven models are powerful solutions for mapping complex webs of relationships among stakeholders, enabling regulators to identify conflicts of interest, high-risk connections, and systemic vulnerabilities. The ECB applied network analytics to identify complex ownership structures, mapping out the interconnections between private equity stakeholders and banks[11]. This enabled the detection of risk clusters that could pose challenges to financial stability

Advances in AI, particularly generative models leveraging graph knowledge bases - such as retrieval-augmented generation architectures - enhance these capabilities. These approaches let regulators analyze interconnected data more confidently as relationships are already built into the graph models, facilitating faster, deeper and more accurate risk identification.

Data Integration

SupTech platforms that integrate external data sources—such as financial industry news, financial disclosures, and sentiment from social media—help enable dynamic risk assessment during licensing. Qatar Financial Centre Regulatory Authority (QFCRA) piloted a social media sentiment analysis[12] tool to detect emerging risks tied to supervised firms. These capabilities could be extended to licensing applicants, offering further insights into reputational and financial risk indicators.

Benefits of SupTech in Licensing and Case Management

- **Efficiency:** Automation reduces delays and accelerates application processing.
- **Accuracy:** Advanced tools minimize errors and enhance decision quality.
- **Scalability:** SupTech adapts to the increasing volume and complexity of licensing demands.
- **Transparency:** Data-driven systems improve documentation, traceability, and trust.

Implementation and Investment Recommendations

Regulators could consider initiating targeted pilot projects, such as implementing NLP or GenAI for document analysis, or deploying risk profiling tools, to gradually build confidence and capacity in SupTech adoption. Exploring collaborative efforts to develop regulation-optimized LLMs may further accelerate progress and enhance the scalability of solutions.

[10] https://documents1.worldbank.org/curated/en/735871616428497205/pdf/The-Next-Wave-of-Suptech-Innovation-Suptech-Solutions-for-Market-Conduct-Supervision.pdf#page=29
[11] https://www.bankingsupervision.europa.eu/press/interviews/date/2024/html/ssm.in240226~c6f7fc9251.en.html
[12] https://www.bis.org/fsi/publ/insights37.pdf

Business Model Analysis

Understanding and evaluating the business models and strategies of regulated entities is essential for maintaining financial stability, protecting consumers and fostering trust in the financial system. As entities increasingly adopt digital-first strategies, diversify revenue streams, and explore innovative products, regulators face growing challenges in assessing the sustainability, risks, and resilience of these evolving business models. SupTech solutions enable regulators to analyze revenue drivers, cost structures, strategic priorities, and emerging risks with greater precision, speed, and depth. Using machine learning, graph analytics, and simulation, regulators can more proactively identify vulnerabilities and ensure firms' business models align with regulatory expectations and desired outcomes.

Revenue and Cost Dynamics: Modeling and Scenario Analysis

Modern financial firms often derive revenue from diverse, and at times opaque, sources, including: Fintech-enabled operations (e.g. embedded finance), high frequency or algorithmic trading, innovative lending and decentralized financial products. Machine learning models analyze revenue streams and cost structures to identify key drivers of profitability and efficiency. These tools can provide predictive insights into how operational or market changes (e.g. economic shocks, shifts in customer behavior, or competitive pressures) may affect firms' financial health.

Simulation tools can enable regulators to test business model resilience under various scenarios, such as the impact of rising default rates or a liquidity squeeze, and/or how consumer shifts to digital-first solutions or green financial products may impact a firm's revenue growth and market share. The Central Bank of Brazil employs predictive modeling to assess non-bank financial institutions' resilience under various scenarios, enabling preemptive action to address potential vulnerabilities[13].

Relationship Mapping: Network and Contagion Analysis

SupTech solutions, particularly graph-based tools and network analytics can help regulators uncover contagion risks - potential pathways for systemic shocks to spreads across firms and financial markets; hidden interdependencies of specific counterparties or revenue streams; and conflicts of interest, which could compromise market integrity or consumer outcomes.

Strategic Alignment and Forward-Looking Indicators

A forward-looking assessment of a firm's strategic direction is essential for understanding its sustainability. SupTech tools enable regulators to analyze public and proprietary data to evaluate strategic priorities, such as expansion into fintech or environmental, social, and governance (ESG)-aligned products, while also monitoring early warning indicators of business model vulnerabilities, like heavy reliance on high-risk products or revenue streams. These tools can help identify misalignment between a firm's business strategies and customer outcomes, such as the inappropriate sale of high-risk products to vulnerable consumers. Additionally, text and sentiment analysis, powered by NLP and LLMs, can extract valuable insights from sources such as public filings, analyst reports, firm disclosures, and customer complaints or feedback data.

Data Integration and Visualization

The increasing complexity of financial products and operations demands integrated and efficient oversight. Modern SupTech platforms aggregate and analyze diverse datasets, including internal supervisory data, such as financial statements and stress test results, alongside external data like macroeconomic indicators, financial market transactions, and social sentiment. Visualization tools and dashboards make these insights accessible, allowing regulators to interpret complex datasets, identify anomalies, emerging risks, and unsustainable practices, and benchmark firms' performance

[13] https://www.bis.org/fsi/publ/insights37.pdf#page=23

and business models against industry peers. The National Bank of Rwanda's Electronic Data Warehouse[14] enables the aggregation of prudential and financial market conduct data, enabling more effective analysis of financial firms' health and business models.

Benefits of SupTech in Business Model Analysis

- **Enhanced Insight:** Advanced analytics provide deeper understanding of financial sustainability.
- **Proactive Risk Management:** Predictive tools identify vulnerabilities before they escalate.
- **Transparency:** Visualization and network analysis improve understanding of complex models.
- **Adaptability:** AI can enable regulators to evaluate emerging business strategies effectively.

Implementation and Investment Recommendations

To strengthen business model analysis, regulators will need to prioritize investments in AI and advanced data analytics. Starting with pilot projects, such as scenario analysis or machine learning for revenue modeling, can provide actionable insights and build institutional capacity. Collaboration with peers can enhance knowledge-sharing and regulators' ability to assess increasingly complex business models.

Assessment of Governance Practices

Effective governance in regulated entities is essential to ensure sound decision-making, risk management, and compliance. Strong governance frameworks help to maintain financial stability, safeguard consumers, and foster trust in the financial system. However, assessing governance practices presents unique challenges for regulators, due to their qualitative nature, fluidity, and the increasing complexity of regulated entities' operations and activities. Governance encompasses multiple elements, many of which can be difficult to quantify, such as leadership, board composition, organizational culture, and risk management structures. Multinational entities face varying governance standards which can create additional challenges and gaps in compliance. As entities adopt digital-first operations and technologies, governance frameworks must also evolve to properly address risks, such as cybersecurity and data ethics.

SupTech can provide data-driven insights into leadership behavior, board dynamics, and organizational resilience, enabling regulators to prioritize and refine their approach to supervision and their interventions with regulated firms.

NLP and Sentiment Analysis

NLP tools can analyze board minutes, audit reports, and leadership communications to assess attitudes toward compliance, risk management, and ethics. Sentiment analysis reveals the tone and context of board discussions, providing insights into the institution's risk appetite and governance culture. For example, the Bank of Thailand has developed a tool[15] to evaluate board minutes from Thai banks, categorizing discussions by topics, time allocation, and board member participation. It provides regulators with a quantifiable view of governance behaviors, highlighting potential red flags like insufficient focus on risk management. Similarly, the Bank of Italy's sentiment analysis tool[16] is applied to board and committee minutes, allowing it to identify governance trends and attitudes, such as overconfidence in risky decisions or neglect of critical risk factors.

[14] https://lab.ccaf.io/wp-content/uploads/2024/03/Cambridge-State-of-SupTech-Report-2023.pdf#page=85
[15] https://www.bis.org/fsi/publ/insights37.pdf#page=21
[16] https://www.bis.org/fsi/publ/insights37.pdf#page=21

Topic Modeling and Anomaly Detection

Automated topic modeling can identify key governance themes, such as risk oversight or diversity, while anomaly detection techniques can help flag irregularities, such as unexplained shifts in focus or the avoidance of significant risks. Anomaly detection models and algorithms including rules-based engines and approaches like isolation forests and auto-encoders - widely used for anomaly detection in areas such as derivatives and payment systems - and more recent advances in RAG-assisted, graph analytics-driven approaches) have demonstrated their value in identifying patterns that deviate from expected norms. These techniques could be adapted to governance-related use cases, helping regulators uncover potential governance anomalies. For instance, a board which fails to discuss information security risks despite increasing external threats, could be flagged for further investigation.

Predictive Risk Scoring for Governance

Machine learning models trained on historical governance data can be used to predict risks associated with current governance structures. These models analyze patterns in features, such as board tenure, leadership stability, diversity, and the frequency or quality of risk discussions, to generate risk scores that help prioritize oversight. By leveraging these models, regulators can identify governance structures that exhibit characteristics associated with heightened risk. For instance, boards with unusually high turnover or prolonged neglect of emerging threats could be flagged for further scrutiny. This data-driven approach allows supervisors to move beyond static governance assessments to a more proactive, risk-based approach.

Benefits of SupTech in Assessment of Governance Practices within FIs

- **Enhanced Visibility:** Tools like NLP and network analysis reveal governance practices and risks that traditional methods might miss.
- **Efficiency:** Automated systems streamline reviews of extensive documentation and governance structures.
- **Proactivity:** Predictive tools identify emerging governance risks, enabling early intervention.

Implementation and Investment Recommendations

Regulators may start with pilot projects such as sentiment analysis of board minutes or machine-learning enabled anomaly detection in governance activities. Investments in data infrastructure and analytics capabilities, paired with collaborative learning from global peers, will ensure governance frameworks remain resilient and adaptable.

Financial and Microprudential Risk Assessment

Evaluating financial risks faced by individual regulated entities is critical for ensuring their stability and resilience. Regulators must address diverse risks, including credit, financial market, operational, and liquidity risks, within an increasingly complex financial ecosystem. Traditional risk models often struggle to capture the interconnections and emerging challenges posed by financial innovation, such as cybersecurity threats, climate risks, and shadow banking. SupTech tools can enhance regulators' ability to assess and monitor risks, providing deeper insights into potential vulnerabilities and enabling timely interventions.

AI-Powered Credit Risk Scoring

Machine learning models, such as random forests and gradient boosting machines, can process large volumes of historical loan data to predict risks across diverse portfolios. These models allow regulators to assess high-risk segments in an entity's loan book, providing early insights into emerging risks. The Central Bank of Brazil's ADAM model[17], uses machine learning to predict borrower defaults, enhancing credit risk assessments of regulated entities.

[17] https://www.bcb.gov.br/en/publications/our_results_2021; and https://www.bis.org/publ/bisbull84.htm

Textual Data for Early Warning Signals

NLP and LLMs applied to financial news, analyst reports, and social media can support detection of financial warning signs in regulated entities. The ECB's Delphi tool[18] leverages NLP to combine financial market risk indicators with information from news sources into a single user-friendly web-based platform. By integrating qualitative and quantitative data, the tool provides valuable insights that help supervisors assess firm-specific risks more effectively.

Stress Testing for Market Risk

Advanced stress testing models can simulate extreme financial market conditions to assess an institution's resilience under adverse scenarios. This allows regulators to evaluate how well an institution can withstand shocks such as sudden changes in equity markets or interest rate hikes. The Bank of England employs neural networks[19] to analyze services inflation, breaking it down into components such as inflation expectations, past inflation dynamics, and international prices. This multi-network model captures complex non-linearities in the data, particularly useful during volatile economic periods. Similar approaches could be applied to stress testing, helping simulate complex scenarios where equity market risks could impact financial institution stability.

Emerging approaches like digital twins, agent-based modeling, and system dynamics modeling—already gaining traction in other industries and among some financial firms—provide regulators with new ways to simulate scenarios and assess how various internal and external factors might impact the financial risk and resilience of individual firms.

Dynamic Liquidity Risk Monitoring

Monitoring liquidity coverage ratios and other key liquidity metrics in real time can allow regulators to maintain a clear view of an institution's liquidity buffers and potential shortfalls. Auto-encoder models, such as those used by the Bank of Canada[20] for retail payment monitoring, could be applied to liquidity risk by detecting anomalies in liquidity flows, providing early alerts when liquidity buffers approach critical thresholds.

Benefits of SupTech in Financial and Microprudential Risk Assessment

- **Improved Accuracy:** Advanced analytics provide more precise risk evaluations.
- **Timeliness:** Real-time monitoring ensures faster detection and response to risks.
- **Scalability:** Automated systems handle growing data volumes and complexity.
- **Proactive Oversight:** Predictive models identify vulnerabilities before they escalate.

Implementation and Investment Recommendations

Regulators could explore SupTech solutions to enhance risk assessment, potentially starting with pilot projects like credit risk scoring or stress testing for liquidity risk. Investments in AI, data integration and simulation techniques offer opportunities to enable more agile and informed oversight.

[18] https://www.bankingsupervision.europa.eu/press/speeches/date/2024/html/ssm.sp240918~522b3441ba.en.html
[19] https://www.bis.org/publ/bisbull84_annex.pdf
[20] ibid.

Macroprudential and Systemic Risk Assessment

Macroprudential and systemic risk assessment focuses on threats that could destabilize the entire financial system. The interconnectedness of financial firms, the rapid pace of innovation, and the global nature of financial markets amplify the potential for systemic crises. Cyber threats, climate-related shocks, and high-frequency trading, further complicate regulatory oversight. Traditional tools often fall short in addressing these challenges, requiring regulators to adopt advanced technologies capable of integrating real-time data, analyzing complex interdependencies, and forecasting systemic shocks.

Real-Time Data Integration and Analytics

Advanced platforms integrate real-time data from diverse financial sources, providing regulators with a comprehensive view of the financial system's health. By aggregating data across institutions and financial markets, these platforms enable the monitoring of liquidity levels, interbank exposures, and financial market volatility as they evolve. Increasingly regulators and others are exploring and embracing the use of "data spaces" to exchange data securely.[21]

Advanced analytics refine this data, uncovering trends and relationships between economic indicators and systemic vulnerabilities, empowering regulators to detect risks early and intervene proactively. By combining neural networks with traditional econometric models, the nowcasting model developed by the Bank of Korea[22] enhances real-time GDP estimates, particularly during periods of economic uncertainty. The use of neural networks allows regulators to better capture nonlinearities in time-series data. The International Monetary Fund[23] has similarly applied a combination of dynamic factor models and several machine learning algorithms to nowcast GDP growth across a heterogenous group of European economies. Through similar techniques, regulators can monitor macroeconomic trends for signals of systemic vulnerabilities.

Predictive Modeling and Early Warning Systems

Predictive models analyze historical and real-time data to forecast potential systemic shocks, while early warning systems monitor key indicators to detect emerging risks. The Central Bank of Ecuador[24] implemented auto-encoder models within its interbank payment system to detect anomalies in payment flows. These models, trained on historical transaction patterns, identified deviations from expected behavior, including both simulated and real-life operational disruptions, such as simulated bank runs. This allowed the central bank to monitor payment system stability in real time, preventing potential liquidity crises.

In collaboration, the Bank of Canada and De Nederlandsche Bank[25] developed auto-encoder models to monitor retail payment transactions. The models were trained to recognize typical transaction patterns, allowing them to detect anomalies that could signal potential liquidity risks, such as sudden shifts in payment flows or withdrawal patterns.

The US Federal Reserve Bank of Cleveland[26] employed the FinBERT NLP model to analyze data within the Beige Book[27]. By extracting sentiment on economic topics like consumer demand, FinBERT has helped the Bank to track shifts in economic conditions and predict potential economic downturns based on the collective sentiment of business leaders. This application of NLP and sentiment analysis can be adapted for early warning systems in macroprudential risk

[21] See for instance https://internationaldataspaces.org/; https://catena-x.net/en/ and https://www.bmwk.de/Redaktion/EN/Dossier/gaia-x.html
[22] https://www.bis.org/publ/bisbull84_annex.pdf
[23] https://www.imf.org/en/Publications/WP/Issues/2022/03/11/Nowcasting-GDP-A-Scalable-Approach-Using-DFM-Machine-Learning-and-Novel-Data-Applied-to-513703
[24] https://www.bis.org/publ/bisbull84_annex.pdf
[25] https://www.bankofcanada.ca/wp-content/uploads/2024/05/swp2024-15.pdf
[26] https://www.clevelandfed.org/publications/economic-commentary/2024/ec-202408-regional-economic-sentiment
[27] The Beige Book, more formally called the Summary of Commentary on Current Economic Conditions, is a report published by the United States Federal Reserve Board of Governors eight times a year. The report is published in advance of meetings of the Federal Open Market Committee. Each report contains a collection of "anecdotal information on current economic conditions" by each Federal Reserve Bank in its district from "Bank and Branch directors and interviews with key business contacts, economists, market experts, and other sources".

assessments. By monitoring market sentiment through news reports, social media, and financial disclosures, regulators can detect emerging systemic risks and act before they impact the stability of the broader financial system.

Scenario Analysis and Stress Testing for System Resilience

Simulation tools model adverse conditions to assess the resilience of the financial system and identify weaknesses in its structure. Such techniques help regulators simulate potential economic shocks and understand how they might propagate through the system.

Benefits of SupTech in Macroprudential and Systemic Risk Assessment

- **Timeliness:** Real-time monitoring provides regulators with immediate insights into systemic vulnerabilities.
- **Proactivity:** Early warning systems and stress testing enable preemptive actions.
- **Visibility:** Advanced techniques bridge gaps between fixed data flows, addressing blindspots.

Implementation and Investment Recommendations

Regulators could initiate pilot projects leveraging nowcasting models and machine learning-based early warning systems to enhance real-time risk detection. Expanding data integration efforts, such as secure "data spaces" for cross-institutional information sharing, can improve systemic oversight. Investing in advanced simulation and stress testing frameworks will enable regulators to model economic shocks more accurately and assess financial system resilience. Collaboration with international peers and research institutions can accelerate adoption, ensuring robust methodologies and best practices in macroprudential risk assessment.

Cyber Risk Detection and Monitoring

Cyber risk has become one of the most significant threats facing society today. As the financial sector increasingly relies on digital platforms and technologies, the potential for cyber-attacks, data breaches, and other cybersecurity incidents has grown. For regulators, the ability to detect and monitor cyber risks is crucial to maintaining the stability and security of the financial system. However, the rapid evolution of cyber threats, driven by increasingly sophisticated and highly-motivated attackers, makes it difficult for traditional regulatory approaches to keep pace. The volume and complexity of data generated by financial firms' digital activities can overwhelm existing monitoring systems, requiring more advanced solutions that can operate at scale, adapt to evolving threats, and integrate data across different sources.

At the same time, regulators face a critical challenge: earning and maintaining the trust of the financial sector in their ability to safeguard the sensitive data they collect. Regulators hold some of the most valuable and sensitive data on the planet—including quarterly reports, exam materials, incident reports, information about firm's strategies and growth ambitions, and resolution planning documents. Addressing this issue requires regulators to modernize their internal security infrastructure, strengthen data governance processes, and enhance examiner training to ensure they can secure sensitive data appropriately and responsibly.

Threat Intelligence and Data Integration

Regulators need timely access to threat intelligence from regulated entities, external feeds, and industry networks to monitor the evolving cyber threat landscape. Effective solutions integrate data from diverse sources, providing a holistic

view of threats and enabling swift responses. These platforms correlate vast amounts of data to identify patterns, detect risks like coordinated attacks, and connect events signaling broader systemic issues.

Threat intelligence platforms offer early warnings by flagging anomalies, such as unusual logins, phishing spikes, or DDoS attacks. Continuous monitoring allows proactive alerts and mitigation strategies, helping regulators act before threats escalate. These technologies ensure vigilant, adaptive risk management in an increasingly digital financial ecosystem.

The Dubai Financial Services Authority (DFSA) launched a Cyber Threat Intelligence Platform[28] to enhance cybersecurity within the Dubai International Financial Centre (DIFC). This platform, developed in collaboration with entities such as the Dubai Electronic Security Center and the UAE's National Computer Emergency Response Team, aims to create a community for sharing information on cyber threats among DIFC businesses. By facilitating the exchange of threat intelligence, the DFSA seeks to bolster the cyber resilience of the financial sector in Dubai.

AI and Machine Learning for Anomaly Detection

AI and machine learning are critical for detecting cyber threats by analyzing large datasets for patterns missed by traditional methods. Behavioral analytics, like User and Entity Behavior Analytics, establish baselines for normal activity and flag deviations, such as irregular logins or data access, to identify insider threats or compromised accounts early. Deep learning models further enhance detection by identifying complex and evolving threats like Advanced Persistent Threats[29] hidden within regular traffic. These models analyze subtle patterns, providing robust defense against sophisticated attacks that conventional systems may overlook.

AI and machine learning are critical for detecting cyber threats by analyzing large datasets for patterns missed by traditional methods.

Automated Incident Response and Orchestration

Swift responses are vital to minimizing the impact of cyber attacks. Automated response systems enable coordinated, timely actions across security layers, reducing reliance on manual intervention. Security Orchestration, Automation, and Response (SOAR) platforms execute predefined actions, such as isolating compromised systems or blocking network traffic, ensuring rapid containment. AI-driven playbooks tailor responses to the specifics of each incident, efficiently addressing minor vulnerabilities or major breaches while minimizing disruption and impact.

CASE STUDY: ASTERisC*: Strengthening Cyber Risk Detection in the Philippines

The Bangko Sentral ng Pilipinas (BSP) developed the Advanced SupTech Engine for Risk-Based Compliance (ASTERisC*)[30] to address growing cybersecurity challenges in the financial sector. This AI-powered tool provides real-time monitoring, risk assessment, and compliance validation, supporting BSP's comprehensive cybersecurity oversight. ASTERisC* continuously analyzes network traffic, system logs, and user behavior to detect anomalies, such as insider threats or sophisticated cyberattacks, before they escalate. Machine learning powers dynamic risk assessments, assigning real-time risk scores to prioritize interventions based on threat severity.

The system also automates compliance checks, ensuring institutions meet cybersecurity standards and address vulnerabilities proactively. By integrating data from financial firms and threat intelligence sources, ASTERisC* enables a unified response to cyber risks across the industry. Since its launch, ASTERisC* has improved early threat detection, allowing BSP and financial firms to mitigate risks swiftly. This proactive approach has strengthened both individual institutions and the financial system's resilience, maintaining consumer trust in an increasingly digital landscape.

---

[28] https://dfsaen.thomsonreuters.com/sites/default/files/net_file_store/200120_DFSA_Launches_Cyber_Threat_Intelligence_Platform.pdf
[29] APTs are prolonged, stealthy cyberattacks by skilled adversaries, targeting specific organizations to steal data, disrupt operations, or conduct espionage.
[30] www.jbs.cam.ac.uk/wp-content/uploads/2024/02/2024-ccaf-state-of-subtech-report-2023.pdf#page=128 and www.centralbanking.com/awards/7958864/cyber-resilience-initiative-central-bank-of-the-philippines

Benefits of SupTech in Cyber Risk Detection and Monitoring

- **Proactive Detection:** Real-time insights identify threats before they escalate.
- **Efficiency:** Automated systems reduce manual workloads and response times.
- **Collaboration:** Secure data-sharing platforms facilitate cross-institutional cooperation.
- **Scalability:** AI-driven models adapt to the increasing volume and complexity of threats.

Implementation and Investment Recommendations

Pilot projects involving anomaly detection or dynamic threat response systems can yield early results. International collaboration and investment in secure data-sharing infrastructure can help to manage cyber threats that transcend borders.

Digital Asset Monitoring and Oversight

Digital assets - cryptocurrencies, tokens, coins, and other distributed ledger or blockchain-based financial instruments - are now prominent within the global financial system. These assets present unique opportunities for innovation and financial inclusion but also present risks related to volatility, fraud, money laundering and financial market manipulation. Traditional oversight methods often fail to address the decentralized, pseudonymous, and borderless nature of digital assets. SupTech solutions provide regulators with advanced tools to enhance transparency, ensure compliance, and mitigate risks in this rapidly evolving ecosystem.

Blockchain Analytics for Transaction Monitoring

Blockchain analytics enhances regulatory oversight of digital assets by providing transparency across decentralized networks. These tools allow regulators to trace digital asset movements and analyze transactions across blockchains. On-chain analytics help visualize asset flows and detect illicit activities like money laundering, fraud, and financial market manipulation. They can also contribute to mitigating sanctions evasion risks and addressing challenges posed by tools like mixers and tumblers. Using advanced algorithms, these platforms aggregate data from multiple blockchains, consolidating transaction histories, including those involving anonymizing services.

Blockchain analytics enhances regulatory oversight of digital assets by providing transparency across decentralized networks.

A key feature is address clustering, which identifies groups of blockchain addresses likely controlled by the same entity. This helps regulators assess broader networks of interactions, assigning risk scores to prioritize investigations. High-risk scores may be flagged for patterns such as darknet interactions or rapid, large transactions bypassing AML controls. Address clustering and risk assessment can be integral to effective digital asset monitoring.

The Bermuda Monetary Authority (BMA)[31] utilizes blockchain forensic tools for anti-money laundering and anti-terrorist financing purposes. They have also explored the use of blockchain data as an early-warning signal for prudential problems. Similarly, HM Government of Gibraltar, through the Financial Services Commission, has partnered with a vendor to implement a blockchain-native AML platform[32] to assist regulatory and law enforcement agencies in

[31] https://www.globalgovernmentfintech.com/global-government-fintech-lab-2023-suptech/
[32] https://www.gibraltar.gov.gi/press-releases/gibraltar-regulatory-agencies-trial-aml-platform-for-crypto-asset-investigations-3322021-6893

combating money laundering and terrorist financing. The platform enables real-time monitoring of high-risk transactions and the tracing of illicit funds using sophisticated visualization tools and proprietary investigative techniques. Employing smart, automated analytics, it addresses complex criminal activities by analyzing transaction patterns, ownership structures, fund sources and destinations, activity fingerprints, e-discovery, and clustering algorithms.

Decentralized Finance (DeFi) Monitoring

DeFi poses unique regulatory challenges because financial activity occurs without traditional intermediaries, instead relying on smart contracts—automated computer programs that execute transactions like lending or trading independently. While smart contracts offer potential efficiencies and transparency, they are not immune to errors or weaknesses in their code, which can be exploited by bad actors. Smart contract auditing tools act like digital "code inspectors," helping regulators review and test the underlying software for potential vulnerabilities or loopholes that could be exploited for fraud, theft, or financial crimes. These tools can also help ensure that the automated processes comply with regulations like Anti-Money Laundering (AML) and Know Your Customer (KYC) requirements, which are designed to prevent illegal financial activity. DeFi monitoring platforms can track metrics like total value locked, liquidity flows, transaction volumes, and decentralized exchange performance. Sudden spikes in activity or liquidity shifts can signal potential exploitation or manipulation.

Artificial Intelligence for Market Surveillance

AI-driven market surveillance is essential for ensuring fairness in volatile digital asset markets. Machine learning models analyze trading data to detect manipulation, such as unusual volumes or price spikes. For example, AI can identify pump-and-dump schemes where prices are artificially inflated before assets are sold off. Sentiment analysis, powered by NLP or LLMs, can be used to assess social media trends, forums, and news articles; enabling regulators to correlate public sentiment shifts with price changes, detecting market manipulation driven by coordinated sentiment campaigns. Combining market surveillance with sentiment analysis allows regulators to proactively mitigate risks in fast-moving digital asset markets.

Cross-Border Collaboration and Information Sharing

Cross-border collaboration is critical for effective oversight of global digital asset transactions. Blockchain-based platforms can enable secure, transparent data sharing between jurisdictions. These systems can provide tamper-proof transaction records, enhancing regulatory cooperation and data integrity. Smart contracts can also support automated reporting by triggering alerts when thresholds are met. For instance, large transactions between jurisdictions can automatically notify relevant regulators. Such real-time systems can enable cross-border monitoring and support swift responses to mitigate risks.

Benefits of SupTech in Digital Asset Monitoring

- **Enhanced Transparency:** Blockchain analytics provide a detailed view of asset flows.
- **Proactive Oversight:** AI-driven tools identify risks before they escalate.
- **Cross-Border Coordination:** DLT and secure computing enable seamless international collaboration.
- **Adaptability:** Advanced analytics address the evolving nature of digital assets and DeFi.

Implementation and Investment Recommendations

The complexities of digital assets necessitate investment in new SupTech capabilities. Pilot projects, such as blockchain analytics for transaction monitoring or sentiment analysis for market surveillance present opportunities for early

impact. Collaboration with international bodies to develop secure information-sharing systems can contribute to tackling the global nature of digital asset risks.

Environmental, Social, and Governance (ESG) Reporting

As entities across society face growing pressure to demonstrate commitment to ESG goals, regulators require transparency, consistency, and accountability in ESG reporting. The challenge is heightened by a lack of uniform reporting standards, diverse data sources, and the unstructured nature of much ESG information. Further complexity results from the need to verify self-reported metrics, detect greenwashing, and benchmark institutions against regulations, industry standards or peers.

Tools like NLP and LLMs help surface insights from unstructured sources such as sustainability reports, press releases, and social media, identifying patterns and inconsistencies. Contextual sentiment analysis helps assess the sincerity and forward-looking intent of ESG commitments. Big data analytics combining traditional and non-traditional data sources—like satellite imagery and IoT streams—can assist with monitoring ESG metrics and predictive modeling can be applied to forecast ESG risks. These capabilities, while crucial, overlap significantly with those required for other regulatory needs, emphasizing the interconnectedness of SupTech applications.

Data Harmonization and Corroboration: The Foundation of ESG SupTech

The fragmented nature of ESG data necessitates robust data harmonization and corroboration across diverse sources and silos. Effective ESG oversight involves combining structured, semi-structured, and unstructured data from internal systems, public disclosures, IoT sensors, satellite imagery, and third-party databases. This complexity drives the need for a modern data platform capable of ingesting, combining, analyzing, and visualizing diverse datasets seamlessly.

A modern data platform[33] integrates unified data governance, scalable data movement, and purpose-built analytics. These features are essential for breaking down silos and creating a cohesive view of ESG performance. For example, integrating data from emissions tracking systems with company disclosures enables cross-referencing and validation. Similarly, visualizing ESG performance at an institutional, sectoral, or regional level provides regulators with actionable insights. Modern platforms also ensure adaptability to evolving ESG frameworks and reporting standards. By harmonizing data formats, they allow regulators to accommodate new metrics without overhauling systems. For corroboration, they facilitate data lineage tracking, offering transparency into the origins, transformations, and usage of ESG data, which is critical for auditing and decision-making.

Purpose-built analytics tools—such as those for geospatial analysis or predictive modeling—empower regulators to extract insights specific to ESG oversight. The ability to scale and tailor these platforms ensures regulators can meet diverse demands, from granular compliance checks to system-wide trend analysis. A unified data approach not only strengthens ESG supervision but enhances broader regulatory capabilities, creating systems that are resilient, adaptable, and fit for purpose.

Case Study Highlight: MAS Project Greenprint

Launched in 2020, MAS' Project Greenprint[34]seeks to enhance transparency in ESG reporting and align financial firms with Singapore's sustainability goals. A key focus is its data infrastructure, using AI and machine learning to monitor

[33] https://aws.amazon.com/blogs/architecture/optimize-your-modern-data-architecture-for-sustainability-part-2-unified-data-governance-data-movement-and-purpose-built-analytics/

[34] https://www.mas.gov.sg/development/fintech/green-fintech#_project-greenprint; and https://sustainablefutures.linklaters.com/post/102i0ff/singapore-mas-and-sgx-launch-further-initiative-under-project-greenprint

environmental impacts in real time. Collaborations with fintech firms have created platforms that integrate big data, enabling institutions to analyze ESG metrics like deforestation and pollution through satellite imagery, enhancing the reliability of self-reported data. The project includes a blockchain-based disclosure platform ensuring secure, tamper-proof ESG data submission. Smart contracts automate checks against sustainability criteria, such as releasing green bond funds only upon meeting emissions targets. Project Greenprint fosters cross-border collaboration among institutions, fintechs, and regulators. Its "ESG Registry" aggregates verified ESG certifications, providing a centralized hub for sustainability data accessible to investors and regulators across the ecosystem.

Benefits of SupTech in ESG Reporting

- **Enhanced Accuracy:** Modern data platforms, NLP, and analytics ensure ESG metrics are validated and standardized.
- **Proactive Oversight:** Predictive models forecast ESG risks, allowing regulators to act swiftly.
- **Holistic Integration:** Unified platforms harmonize data across silos for comprehensive ESG insights.

Implementation and Investment Recommendations

Modern data platforms can unify ESG data sources and support evolving standards. Pilot projects, such as predictive analytics for emissions tracking or NLP for analyzing unstructured data, offer immediate benefits. Initiatives like MAS's Greenprint demonstrate the potential of integrating DLT and advanced analytics for transparent and accountable ESG reporting.

Regulatory Reporting and Data Collection

Regulatory reporting and data collection are fundamental processes for financial regulators, enabling them to monitor the health of regulated entities, ensure compliance with regulations, and make informed decisions to safeguard financial stability. The growing complexity of financial instruments, coupled with the globalization of markets, has resulted in an exponential increase in data volume and diversity. Traditional processes struggle to keep pace, introducing risks of delays, errors, and inefficiencies. Regulators now face heightened demands for real-time or near-real-time data to address the rapid evolution of financial markets, alongside the critical need to ensure data security and integrity. Safeguarding sensitive information from cyber threats while maintaining accuracy and reliability is essential for enabling timely, effective oversight in today's interconnected financial ecosystem.

SupTech solutions can streamline data collection and reporting through automation, advanced analytics, and seamless integration, allowing regulators to process vast datasets efficiently, maintain data quality, and ensure compliance.

Automated Data Collection and Integration

Automated tools can streamline the collection of structured and unstructured data, reducing errors and delays while improving the timeliness of regulatory reporting. Application Programming Interfaces (APIs) enable financial firms to submit transaction data and risk metrics in real time, ensuring consistency across reporting frameworks. These systems eliminate manual processes that can introduce errors, allowing for continuous, high-volume data collection. Web scraping tools complement this process by gathering additional information from public disclosures, market reports, and other external sources. This automated cross-verification allows regulators to validate self-reported metrics against independent data, enhancing the reliability of the information used for oversight. By integrating these technologies, regulators can achieve a comprehensive and up-to-date view of financial markets with minimal human intervention.

Data Standardization and Transformation

Ensuring data from diverse sources is standardized and ready for analysis is critical for effective oversight. Extract, Transform, Load (ETL) platforms play a pivotal role, converting raw data into uniform formats while flagging discrepancies for review. Large Language Models (LLMs) enhance these capabilities by processing unstructured data, such as narrative reports or press releases, extracting metrics, and summarizing documents into actionable insights. Metadata management platforms boost transparency by tracking data lineage, documenting origins, transformations, and usage throughout the data lifecycle. Holistic data standardization approaches help regulators harmonize information, supporting consistent and accurate analysis.

AI-Powered Data Validation and Reporting

AI can enhance the quality and utility of regulatory data by validating inputs and automating report generation. Machine learning models, such as anomaly detection algorithms can identify irregularities in submitted data—like unexpected spikes in liquidity metrics—enabling timely interventions. These tools enhance accuracy and reduce oversight risks. Natural Language Generation tools can convert structured datasets into coherent reports, highlighting risks and trends with precision.

Case Study Highlight: FINRA's regulatory reporting, data management and advanced analysis at massive scale

The Financial Industry Regulatory Authority (FINRA)[35] operates one of the most sophisticated cloud-based systems for regulatory reporting and data management, overseeing the activities of U.S. brokerage firms and exchange markets. Processing over 100 billion daily market events, FINRA uses real-time surveillance and analytics to detect market misconduct, such as insider trading and manipulation, ensuring investor protection and market integrity. FINRA's system efficiently handles massive data volumes, leveraging machine learning and predictive analytics to identify unusual trading patterns, detect fraudulent activities, and flag market anomalies. By combining real-time monitoring with historical data analysis, FINRA proactively mitigates risks and ensures compliance. The system's cloud-based architecture provides scalability, allowing it to adapt seamlessly during periods of increased market activity or volatility, ensuring uninterrupted data processing and robust surveillance.

Security and reliability are central to FINRA's operations, with encryption, strong protocols, and disaster recovery mechanisms safeguarding data integrity. Additionally, using a common, open, and well-defined data format, which standardizes the exchange and storage of information, enables seamless integration of data from diverse sources. The lightweight, flexible structure of such standards supports efficient processing and analysis, accommodating the complexity of FINRA's datasets while ensuring compatibility, transparency, and adaptability. The adoption of open, standardized formats also enhances interoperability and facilitates efficient communication with external systems, streamlining reporting to other regulatory bodies.

Benefits of SupTech in Regulatory Reporting

- **Efficiency:** Automation reduces manual workloads and improves data submission accuracy.
- **Proactive Oversight:** Real-time processing and anomaly detection allow timely interventions.
- **Scalability:** Cloud-based systems handle increasing data volumes with ease.
- **Enhanced Transparency:** Metadata tracking ensures data integrity and traceability.

[35] https://aws.amazon.com/blogs/publicsector/finra-cat-selects-aws-for-consolidated-audit-trail/

Implementation and Investment Recommendations

To modernize regulatory reporting, regulators are investing in SupTech solutions that automate data collection, validation, and analysis. Pilot projects, such as deploying APIs for continuous data submission or adopting anomaly detection models, can deliver immediate benefits. Collaboration on standardized data frameworks will further enhance global interoperability.

Investigation and Enforcement of Regulatory Violations

Investigation and enforcement of regulatory violations are essential to maintaining the integrity of the financial system. As financial services become increasingly digital, complex, and global, regulators are confronted with an ever-growing volume of data and the use of sophisticated tactics to conceal non-compliance. This complexity makes detecting, investigating, and enforcing regulatory violations more challenging. Many financial transactions occur in real-time, across borders, involving highly interconnected markets and actors. Traditional investigation processes cannot keep pace with the rapid evolution of both financial products and the associated compliance risks. Moreover, as financial firms and their services become more reliant on digital infrastructure, new risks—such as cybersecurity threats, data breaches, and digital fraud—require advanced detection tools. Slow manual investigations can lead to delays in enforcement actions undermining their deterrent effect and eroding public trust in regulatory authorities.
Effective enforcement requires swift and accurate identification of violations, coupled with transparent and consistent action. Regulators must therefore turn to advanced technologies, including artificial AI, machine learning (ML), and automation, to enhance their ability to investigate violations and take decisive action. The integration of these technologies is crucial for achieving credible deterrence and maintaining the stability of the global financial system.

Advanced Surveillance and Detection Systems

The growing complexity of financial transactions and digital financial services has made near real-time surveillance essential. Advanced systems using machine learning, deep learning, and analytics can detect irregularities before they escalate into major regulatory issues. By continuously monitoring transaction flows, financial data, and institutional behaviors, such systems enable earlier detection of potential violations, allowing for timely regulatory action.

Machine learning algorithms are central to predictive analytics, identifying anomalous patterns such as unexpected transaction spikes or frequent interactions with high-risk accounts. Deep learning models can monitor user behavior across financial networks, spotting deviations that may indicate money laundering or fraud. Regular updates to detection mechanisms ensure adaptability to emerging fraud techniques and cybersecurity threats. NLP further enhances oversight by analyzing unstructured data, such as emails and chat logs, for signs of insider trading or collusion. Combined with graph-based analytics, regulators can map relationships within financial networks, exposing connections that could signal coordinated regulatory breaches. This multi-layered approach delivers deeper insights into financial misconduct.

Automated Investigation Tools

After identifying potential breaches, regulators require automated tools to conduct investigations efficiently and accurately. AI-powered systems can aggregate and analyze large datasets, accelerating inquiries and reducing human error. AI-driven case management systems consolidate transaction records, communication logs, and reports, creating a unified view of incidents. Machine learning models can support prioritization of high-risk cases based on past violations or risk parameters, enabling targeted scrutiny.

Digital forensics tools enhance investigative capacity by recovering and analyzing hidden or deleted data. These tools are vital in cases of cybersecurity breaches or insider trading, where evidence is often deliberately concealed. By tracing data to its origin, regulators can uncover key actors and patterns linked to breaches. Predictive analytics tools add a proactive dimension, using historical data to forecast future violations. By identifying trends that suggest recurring non-compliance, regulators can intervene early to prevent escalation and reinforce market stability and trust.

FINRA's Knowledge Graphs for Regulatory Investigations and Consolidated Audit Trail

The Financial Industry Regulatory Authority (FINRA) has pioneered the use of knowledge graphs to represent the intricate web of transactions, entities, and relationships in the securities markets[36]. By creating knowledge graphs, FINRA's investigation teams can visualize complex financial interactions, helping them identify potentially fraudulent activities, insider trading, or unusual trading patterns that might otherwise be missed. To construct these knowledge graphs, FINRA implemented a document processing pipeline powered by machine learning models for text recognition and entity identification. By leveraging tools such as NLP and graph databases, FINRA can process large volumes of text from multiple documents, linking relevant data points into a cohesive and actionable network. The solution effectively captures relationships between individuals, entities, and transactions, giving FINRA investigators the ability to trace financial flows with increased accuracy and speed.

Financial Conduct Authority's (FCA) Machine Learning for Insider Trading Detection

The FCA employs machine learning algorithms to improve insider trading detection in U.K. financial markets[37]. Handling around 150 billion data points annually, the FCA's systems monitor transactions, communications, and other behaviors to detect suspicious patterns indicative of insider trading. These tools analyze vast data volumes, flagging anomalies for investigation. Machine learning models trained on historical data recognize subtle patterns, such as trade timing around earnings announcements or mergers, enhancing the regulator's ability to detect unlawful activity on a larger scale than manual reviews. By refining its models, the FCA has improved the speed, efficiency, and accuracy of its investigations.

HKMA's Network Analytics Solution for Combating Financial Crime in Instant Payment Systems

The Hong Kong Monetary Authority (HKMA[38]) has implemented a network analytics solution in response to the growing threat of financial crimes, particularly in the context of instant payment systems. Instant payments, while enhancing the efficiency and convenience of financial transactions, have also created opportunities for criminal activities such as fraud and money laundering. The speed at which these transactions occur makes it difficult for traditional surveillance methods to detect and effectively address suspicious behavior.

HKMA's network analytics solution uses graph-based analysis to map and analyze complex relationships within the financial ecosystem. By visualizing these relationships, it helps regulators identify patterns that may indicate suspicious activities, such as clusters of transactions without clear business rationale. The tool integrates data from various sources, including transaction data, user activity logs, and external intelligence feeds, to create a comprehensive view of financial networks. This multi-dimensional approach helps regulators spot unusual activities and understand their broader context. For instance, the system can flag transactions that seem innocuous in isolation but collectively indicate fraud or money laundering.

[36] https://d1.awsstatic.com/events/Summits/amer2021/maysummitonline/FINRAs_knowledge_graphs_improve_regulatory_investigations_WPS204.pdf
[37] https://www.fca.org.uk/publication/documents/from-maps-to-apps.pdf
[38] https://www.jbs.cam.ac.uk/wp-content/uploads/2024/02/2024-ccaf-state-of-subtech-report-2023.pdf#page=120

Benefits of SupTech in Investigation and Enforcement

- **Efficiency:** Automated tools streamline investigations and reduce manual workloads.
- **Proactive Oversight:** Predictive models identify violations before they escalate.
- **Enhanced Precision:** Real-time data and analytics enable targeted enforcement.
- **Scalability:** SupTech solutions adapt to increasing data volumes and complexities.

Implementation and Investment Recommendations

Regulators increasingly need to leverage advanced surveillance, detection, and investigation tools to stay ahead of increasingly sophisticated financial crimes. This includes embracing AI-powered anomaly detection, real-time data monitoring, and automated investigative processes to enhance efficiency and accuracy in identifying breaches.

CONCLUSION

As the financial landscape continues to evolve, so too must the regulatory approaches that ensure its integrity, resilience, and inclusivity. The advent of digital financial services has brought transformative benefits, expanding access to the unbanked and accelerating innovation. Yet, these advancements also introduce significant risks, including heightened exposure to fraud, systemic vulnerabilities, and regulatory challenges that span borders and jurisdictions.

SupTech can represent a critical tool for regulators striving to address these dual imperatives. By integrating advanced technologies—such as artificial intelligence, machine learning, blockchain analytics, and real-time monitoring—SupTech can enhance the capacity of regulatory agencies to supervise increasingly complex financial ecosystems effectively. These tools not only streamline traditional regulatory processes but also enable proactive, data-driven decision-making, fostering an environment where innovation and resilience can coexist.

This paper has outlined key capabilities and best practices for SupTech implementation, offering practical guidance to regulators. From automating licensing processes and enhancing business model analysis to improving governance oversight and strengthening cybersecurity, SupTech's potential to modernize regulatory functions is vast. Equally important is its role in addressing emerging challenges, such as the rise of digital assets, environmental, social, and governance oversight, and the growing threat of sophisticated financial crimes.

The road to a fully modernized regulatory framework is challenging but achievable.

However, realizing the full potential of SupTech requires more than technological adoption. It demands a strategic vision aligned with regulatory goals, a commitment to fostering collaboration and knowledge-sharing, and a culture of experimentation and agility. Regulators must balance innovation with security, adapt to rapid changes with iterative approaches, and treat data as a core organizational asset.

Looking ahead, collaboration among regulators, financial firms, and global peers will be essential. Shared insights, co-developed solutions, and mutual learning can accelerate SupTech adoption and enable consistent, effective oversight across borders. By embracing this transformative opportunity, regulators can safeguard financial stability, enhance trust, and enable a financial ecosystem that is not only innovative but also equitable, transparent, and resilient.

The road to a fully modernized regulatory framework is challenging but achievable. Through strategic investments, thoughtful integration of technology, and unwavering commitment to public trust, regulators can position themselves as stewards of a future-ready financial system, capable of navigating the complexities of the digital age.

The author would like to thank the following AWS colleagues for their collaboration on this paper: Saket Narayan, Laurent Domb, Denyette DePierro, Mehmet Akyuz, Sally Peck and Katherine Velos.