VIEW POINT

CLOUD COMPUTING AND THE FUTURE OF FINANCIAL CRIME MANAGEMENT

Abstract

The digitization of the banking and financial services industry has seen an alarming increase in cases of financial crimes. Organisations are now heavily investing in financial crime management solutions that are leveraging Regulatory Technologies (RegTechs) such as machine learning, natural language processing, robotics process automation, and big data to name a few. This paper discusses how cloud-based risk management is a clear winner to address the challenges one may encounter while combating financial crime.

Infosys®
Navigate your next

The depth of financial crimes

The onset of the digital age has seen an unpredictable shift in financial crimes around the world. Case in point, the banking and financial services industry (BFSI) has been plagued by financial crimes and sure enough, all of them end up bleeding sensitive data with innocent people bearing the brunt.

The inefficacy of traditional methods of detecting fraudulent activities such as establishing policies and internal controls, conducting regular training, and monitoring financial activities have persuaded organizations to significantly invest in developing sophisticated crime detection, prevention, and deterrence capabilities. There are now improved financial crime management solutions available in the market. Though, for the same reason, the perpetrators of these crimes have advanced in their techniques too. They are adopting highly sophisticated methods to commit financial crimes. The existence of chat rooms, the dark web, and cryptocurrency, along with data acquired through phishing, vishing, and other malware have allowed perpetrators to connect, coordinate and perform complex, heavily layered transactions. These transactions are extremely difficult to detect and trace. However, despite businesses investing in these programs and committing time and money, there are still miles to go in the fight against financial crimes.

The industry has increasingly seen cases of terrorist financing (TF) and money laundering (ML), among other crimes such as identity theft, tax evasion, embezzlement, forging, and counterfeiting. They are major threats to the social order, undermining coordinated worldwide efforts to tackle crimes like environmental destruction, and human, wildlife, and drug trafficking. According to Forbes' Anti-Money Laundering (AML) Fines 2021 Report, financial institutions were fined a staggering $2.7 billion for AML failings & compliance breaches.[1] While a mid-sized bank spends nearly US$ 48 million per year on AML compliance, a lot of work remains to be done, as is evident from the increased actions from law enforcement agencies and regulators caused by high-profile scandals linked to the perpetuation of financial crime.[2]

1. <https://www.forbes.com/sites/forbestechcouncil/2022/03/24/lessons-from-the-seven-largest-aml-bank-fines-in-2021/?sh=341d4ec08ced>
2. <https://home.kpmg/mc/en/home/insights/2019/03/combating-financial-crime-fs.html>

The role of RegTechs in financial crime

Regulatory technology (RegTech) is the application of emerging technologies such as machine learning, natural language processing, blockchain, and artificial intelligence (AI) to improve the way businesses manage regulatory compliance. It has been rapidly maturing, with firms leveraging it for regulatory monitoring, reporting, and compliance.

These RegTechs leverage one or more real-time data-aggregation platforms using fuzzy logic, rapid automation, and text and voice analytics to create a better balance between risk, costs involved, and the associated outcomes, thereby addressing the below areas that render the existing compliance processes insufficient:

- Inferior quality of data and a high rate of false positives
- Non-standard processes, fragmented systems & platforms
- Lack of standard and focused reporting
- Lack of robust real-time detection and prevention

RegTechs not only help prevent compliance breaches, which save financial institutions from paying hefty fines to the regulatory authorities but also find their application in financial crime detection.

RegTechs can help in the following ways with financial crime detection:

1. **Machine Learning (ML)** using random forest, gradient boosting, and deep learning, helps capture the subtleness and dynamism of criminal behaviours that are nearly impossible to code under a rules-based approach. ML finds its uses in customer screening, transaction monitoring, knowing your customer (KYC), Customer Due Diligence (CDD) & Enhanced Due Diligence (EDD) to name a few.
2. **Natural Language Processing** is another cognitive solution that uses sentiment and text analysis to highlight a particular emotion and map past behaviour. From an Anti-Money Laundering (AML)/ Combating the Financing of Terrorism (CFT) perspective, it allows organisations to gain insight into actual frauds or intents to fraud and take appropriate action either pre-emptively or reactively.
3. **Robotic Process Automation (RPA)** finds use in resource-intensive tasks such as document classification and data extraction, name screening, KYC verification, and data entry due to their routine, and rules-based nature.
4. **Big Data/Data analytics** uses advanced algorithms to process large volumes of diverse data from a variety of sources to uncover patterns and relationships in consumer behaviour, which increases the chances of spotting cases of ML or TF.
5. **Privacy Enhancing Technology (PET)** is used in analysing data hosted in a secure environment to provide reports without disclosing any sensitive information, enabling FIs and AML/ CFT regulators to share information without the risk of data breaches. This facilitates greater access to information and supports collaboration on financial crime risk intelligence.

Cloud-based financial crime management

The pressing need to process vast volumes of data in a shorter amount of time, with staff and budget constraints, multiplies the chances of error and compounds the risk. Cloud computing has proven useful in this area, providing a way to address these challenges to combat financial crime and improve compliance. Safe to say, of all banking activities, financial crime management is an area that can benefit immensely from cloud computing.

» **Processing large and complex data sets:** Cloud computing allows seamless integration of all data sources to create a lone source of truth, by eliminating data silos' blind spots, resulting in cleaner, context-specific data structures. This enables the risk teams to focus on analysis and insights.

» **Lack of enough computing power:** Cloud deployment models not only offer the required computing power to run such sophisticated AI/ML models, but also provides the flexibility to scale up as per need. Cloud systems also have inbuilt, ready-to-use libraries that can be accessed to increase the effectiveness of the existing capabilities.

» **Big data, and analytics all in one place:** Cloud-based utilities for reference data that involve gathering, cleansing, standardizing, and maintaining a copy of all data, allow centralized investigations of customer events across business functions and the customer lifecycle for enhanced due diligence and sufficient case resolution.

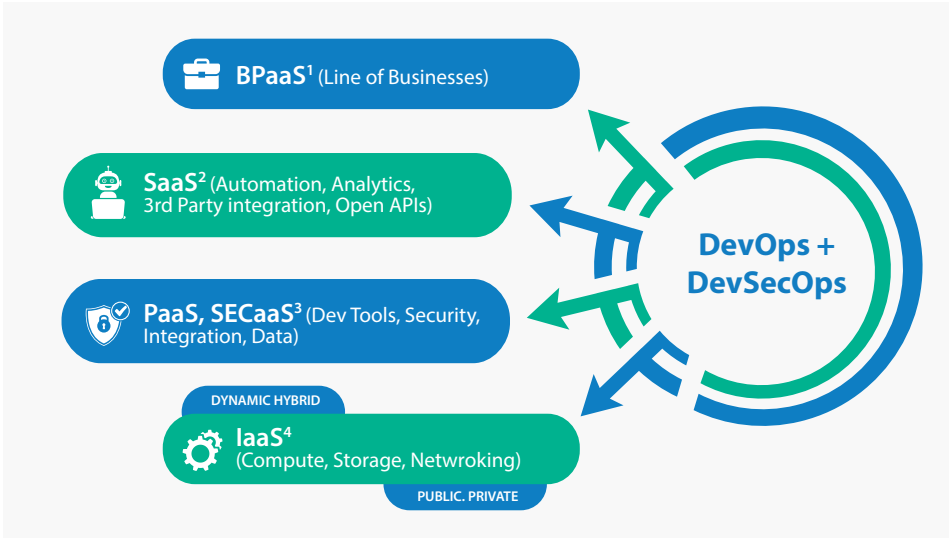
» **An end-to-end solution suite:** Cloud provides an end-to-end suite of applications for regulatory compliance and fraud deterrence, which caters to all financial risk management needs by bringing them under one umbrella as a service.

» **Equipping business with appropriate tools:** Easy to configure cloud-based solutions with out-of-box configurations enriched with inbuilt tools for designing complex scenarios, analysis, and threshold simulation, help business units run simulations on various scenarios to risk assess the portfolio. This not only helps with a better understanding of the risks they are running but also gives them a sense of ownership over their risk decisions.

Cloud-based financial crime management

The substantial advantages of cloud computing come with their own set of challenges while migrating the risk management systems and activities from on-premises to the cloud. A clear transition path that addresses the complexity, cost, culture, and new capabilities, must be managed effectively by aligning them with the larger enterprise migration.

The first step towards cloud migration would be to choose the right operating model that will allow the organisations to benefit from the flexibility, agility, and scalability of both technology and business operations. The ideal cloud-based operating system would consist of infrastructure, platforms and security solutions layering on top of each other to form a powerful model, as depicted in the image below. The key tenets of the model would allow seamless integration of business operations and ops transformation through agile DevOps and DevSecOps on top of robust platform security.



[1]BPaas = business process as a service

[2]SaaS = software as a service

[3]PaaS, SECaaS = platform as a service, security as a service

[4]IaaS = Infrastructure as a service

The second step would be to prioritize the use cases/functions that would be part of the phased migration journey. Each use case should be identified based on their feasibility determined by facets such as volume, complexity, external integrations, cost-benefit, and ease of migration. The early phases should comprise the quick wins, with the more complex and risqué functions going in subsequent phases basis the confidence achieved from the earlier migrations. Proper analysis and phased migration will not only establish an efficient risk management framework on the cloud but also ensure that the process does not become too overwhelming and leave out loopholes for the entire framework to fall apart.

Way forward

The benefits of cloud-based risk management are too good to be ignored by regulators and organisations. Financial institutions are finding that cloud computing is quickly becoming a necessary part of the risk management function. An organization's ability to quickly adapt, pre-empt and respond to the evolving nature and the increasing number of risks, which forms the cornerstone of cloud computing, will determine the future of financial crime prevention. Organizations that choose not to embrace cloud computing pose a notable risk to themselves and the economy.

References

1. https://www.ibm.com/downloads/cas/ZEPGYEWR#:~:text=With%20cloud%20computing%2C%20there%20is,significant%20up%2Dfront%20capital%20expenditure.

2. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/building-a-cloud-ready-operating-model-for-agility-and-resiliency

3. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-transforming-financial-crime-management-through-technology-280521.pdf

4. https://www.forbes.com/sites/forbestechcouncil/2022/03/24/lessons-from-the-seven-largest-aml-bank-fines-in-2021/?sh=341d4ec08ced

5. https://home.kpmg/mc/en/home/insights/2019/03/combating-financial-crime-fs.html

Authors

Subhro Modak
Senior Consultant, Digital Transformation Services, Infosys BPM

Subhro is a consultant with 10+ years of industry experience in the financial services and banking domain. His core areas of expertise are program management, digital transformation, and business analysis across retail and wholesale banking. Subhro has driven various initiatives and complex large-scale programs across retail banking (account services) and wholesale banking (forex and corporate services) processes. His current role involves working on consulting engagements in the banking domain and leveraging technology to improve operational efficiency and user experience.

Prior to Infosys, Subhro worked with Axis Bank, Altisource Business Solutions, and State Bank of India, in diverse roles.

Sourav Ghosh
Senior Industry Principal, Infosys BPM

Sourav is a Senior Industry Principal with Infosys BPM's Digital Transformation Services, responsible for Industry Solutions – Digital Solution Design and Delivery. An IBM-certified Design Thinking practitioner, he advises organizations on their operations strategy, assists them in improving the profitability and efficiency of business processes, and helps in executing business transformation through the calibration of operating models and technology.

Prior to Infosys, Sourav had been with IBM, Satyam, Tata Consultancy Services, and Standard Chartered Bank across a variety of roles in India, the U.S., and the U.K.

* For organizations on the digital transformation journey, agility is key in responding to a rapidly changing technology and business landscape. Now more than ever, it is crucial to deliver and exceed on organizational expectations with a robust digital mindset backed by innovation. Enabling businesses to sense, learn, respond, and evolve like a living organism, will be imperative for business excellence going forward. A comprehensive, yet modular suite of services is doing exactly that. Equipping **organizations with intuitive decision**-making automatically at scale, actionable insights based on real-time solutions, anytime/anywhere experience, and in-depth data visibility across functions leading to hyper-productivity, Live Enterprise is building connected organizations that are innovating collaboratively for the future.

For more information, contact infosysbpm@infosys.com

Infosys®
Navigate your next