Infosys
Navigate your next

FINANCIAL SERVICES RISK AND COMPLIANCE TRENDS IN THE POST-PANDEMIC WORLD

Infosys | Knowledge Institute

Contents

Rajneesh Malviya

Senior Vice President,
Financial Services, Infosys

Ashok Hegde

Vice President,
Financial Services, Infosys

Amit Khullar

Head, Risk and Compliance,
Financial Services, Infosys

Foreword

Risk and compliance within financial services have been undergoing transition. After the 2008 global financial crisis, supervisors and regulators across the world were focused on ensuring the financial resilience of firms. However, the spotlight is now shifting towards the firms' non-financial risks.

Several developments are shaping this shift in focus. The uptake of emerging technologies such as AI/ML and cloud is growing as these bring in substantial business benefits. Yet, they also create new risks and vulnerabilities. The rise in cybersecurity incidents and data breaches, the onslaught of novel and sophisticated financial crimes, the rising obsolescence of legacy IT, and the growing dependence on third-party service providers have increased operational risks for financial institutions. As per a LexisNexis study, for every dollar of fraud loss, financial institutions now incur US$3.25 in costs. These charges include investigation cost, fines and legal fees, transaction face value, and interest.

The COVID-19 outbreak has compounded the operational challenges to financial institutions and is testing their operational resilience. Many other facets of risk and compliance, including credit risk management, financial crime risk management, and regulatory compliance and reporting, have been impacted as well. The outbreak has elevated the risks to banks' loan portfolios. There has also been a spurt in digital financial crime including phishing emails linked to the epidemic. The pandemic has forced regulators to postpone the implementation dates of key mandates such as Basel III.

Climate change related risks are a growing concern for financial institutions. The year 2019 witnessed multiple storms and wildfires across the globe including the Australian bushfire, and Typhoon Hagibis in Japan. Apart from their economic impact, such events raise the financial risks for banks.

Over the next few years, we expect regulatory scrutiny of firms' operational resilience to intensify. Financial institutions will have to conduct comprehensive stress tests to demonstrate their preparedness for managing any operational disruptions. Maintaining business continuity, mitigating cyber risks, preventing IT outages, ensuring system and data access and availability, managing IT obsolescence, and strengthening third-party risk management (TPRM) are amongst the key areas that will be scrutinized.

It is highly unlikely that any new regulations will be introduced over the next few months by global governing bodies such as the BCBS or FSB. However, ongoing regulatory initiatives, such as FRTB implementation or LIBOR transition, would continue to be on the regulators' radar.

In this 2020 edition of our report, we have covered some of the key trends in the financial services risk and compliance domain that we believe will play out in the next few quarters.

BUILD OPERATIONAL RESILIENCE, AND KEEP PACE WITH EVOLVING RISKS

Financial institutions have intensified their focus on building operational resilience. Firms are bolstering their capabilities to effectively manage newer risks such as those related to digital technologies, cyber and data security, third-party risks, pandemics and climate change.

On their part, regulators too are increasing their scrutiny of financial institutions' operational resilience. They are broadening their earlier BCP/DR focus to include all aspects of firms' operational and cyber resilience. Regulators are also evolving the regulations to keep up with digital crime. Further, they are encouraging firms to leverage digitization and automation to fight financial crime and strengthen their operational resilience.

Trend 1: Strengthen operational resilience with technology

Operational resilience helps financial institutions better respond to and recover from disruptions of business operations, customer segments or even the industry at large. Regulators and supervisory agencies, historically focused on building financial resiliency, now have dived their attention to building operational resiliency as well. A regulatory push, increased digitization, and a need to plan for uncertain events have contributed to institutions increasing focus on operational resilience.

Regulators such as the EBA, BOE, FCA, PRA and FRB, are focused on building financial institutions' operational resilience, in addition to their financial resilience. Institutions are also being closely scrutinized on these fronts. The agencies are also concentrating on the operational robustness of institutions and the technology they use. In the U.S., the FRB is conducting horizontal examinations to gauge financial institutions' operational resilience.

Rapid technology evolution and digital disruption have increased the need for building operationally robust systems. Increased digital adoption has also paved the way for a rise in cybercrime and cybersecurity incidents. Interconnected interfaces that collaborate with third party platforms have created new vulnerabilities in systems. For example, the EBA has published its guidance on security, information and communications technology risk management for banks. Despite a rise in incidents, digital is a must as customer expectations have increased. Customers now expect "anytime-anywhere" banking, real-time processing, and omnichannel experiences without technical glitches.

Unforeseeable events such as COVID-19 and natural disasters including climate change demand novel strategies that ensure operational resilience. These include strategies for remote workforce management, data security assurance, managing supply chain disruptions and business continuity. In the wake of the COVID-19 crisis, financial sector authorities have recommended that international actions to define the operational resiliency standards should take into account (a) employee safety; (b) infrastructural needs of the critical employees to support key business services; (c) IT capacity, scalability and flexibility; (d) information security and cyber resilience; and (e) the operational continuity of critical third-party service providers.

Steps to build operational resilience

Financial institutions have been undertaking the following actions to strengthen their operational resilience:

Reinforcing strategic thrusts

Institutions are revising their operational resilience program to make it comprehensive, adaptable and forward-looking. They are also strengthening the synergy between their operational risk management (ORM) and business continuity management (BCM) functions. This helps reinforce the links between key functions such as risk, compliance, corporate functions and LoBs. These programs ensure active involvement of boards and senior management, in turn helping prioritize operational resilience programs and related investment decisions.

Third party resiliency

Institutions are increasingly trying to understand the risks and operational resilience of third-party providers such as back-office service providers, IT service providers and cloud solution vendors. Financial institutions are also strengthening their vendors' due diligence processes. Institutions are identifying opportunities to collaborate with providers to strengthen the providers' risk management practices and information sharing mechanisms.

IT systems

To strengthen their IT systems' resilience, institutions are either retiring or replacing obsolete legacy systems to ensure minimal operational disruption. This involves bolstering data management and cybersecurity.

Business continuity and disaster recovery (BCDR)

Institutions are strengthening their BCDR plans by better understanding their IT systems' vulnerabilities and mission-critical operational processes.

Stress testing

Financial institutions are focusing on scenario analysis, threshold identification, comprehensiveness of tests, and response planning to strengthen the scenario-based stress testing of their operational resilience.

Actions taken by financial institutions to build operational resilience

Lloyds Banking Group has committed to invest £3 billion in technology. The group has been working for over the past two years to institute a digital office program. It is leveraging Microsoft's cloud platform to improve operational resilience, enhance business agility, and offer on-demand scalability across the group. It is offering several productivity tools within Office 365 to all its employees. The group is also rolling out Microsoft Managed Desktop across its business — making it the world's biggest FI to do so.

In 2019, the Bank of Canada launched the Canadian Financial Sector Resiliency Group (CFRG) to strengthen the operational and cyber resilience of Canada's financial sector. Amongst other activities, the CFRG was set up to support the ongoing operational resiliency initiatives such as benchmarking exercises and regular crisis simulation. The central bank has also made significant investments to enhance its own operational redundancy and resilience to withstand major disruptions, including natural disasters and cyber-attacks.

The World Federation of Exchanges (WFE), a global industry group for CCPs and exchanges, has provided details of measures taken by the industry to enhance cyber resilience during COVID-19. As per the group, several CCPs and exchanges have activated their business continuity plans to ensure their operational resilience. Actions taken include mass remote working and collaboration, and third-party risk management measures to facilitate efficient and safe trading during the pandemic. Through the WFE, these financial institutions have also been collaborating and sharing best practices to increase operational resilience.

Trend 2: The FCRM space is evolving dynamically

Recently several factors have led to a rise in financial crimes including fraud, cyber-crime, money laundering, trade abuse, market manipulation, terrorist financing and tax violations. As per a 2020 survey, around 50% of the respondents said that they had experienced fraud within the previous 24 months. During the same period, the reported losses from fraud amounted to US$42 billion. According to research, globally money laundering related crimes cost enterprises between US$1.4 trillion and US$3.5 trillion annually.

Factors contributing to a rise in financial crimes

- Increase in digital payments volumes and the rapid evolution of online and mobile payments channels such as alternative payments providers (PayPal, Google Pay, Apple Pay, Skrill, Square, Stripe), social applications, and electronic gift cards.
- Security vulnerabilities of the newer digital technologies such as cloud, mobility, social, etc.
- Rise in the execution of sophisticated crimes by fraudsters and fraud rings such as advanced persistent threat campaigns (for example Carbanak), identity theft, distributed denial-of-service attacks, ransomware, SIM swap fraud, infiltrated POS systems, and man-in-the-middle fraud.
- New avenues for financial crime including (a) casinos and online gaming zones on luxury cruise, (b) exploiting the anonymity feature of virtual currencies (bitcoin), etc.

The COVID-19 crisis has provided fraudsters with another avenue for perpetrating crime. For example, UK's Action Fraud has been receiving thousands of reports of phishing emails linked to the pandemic. Criminals have been targeting vulnerable citizens by acting as sellers of face masks, or pretending to be from WHO or the CDC, and carrying out malware and phishing attacks.

The financial crime risk management (FCRM) sphere has been evolving rapidly. Here are some of the changes being witnessed:

Rise in regulatory expectations

Regulators are taking steps to strengthen financial institutions' FCRM practices. For example, in Europe, EU member states must transpose the 6th Anti-Money Laundering Directive (6AMLD) into national law by December 3, 2020. The 6AMLD brings in significant changes such as more stringent punishment for money laundering, and stricter measures for virtual currencies. Similarly, in Australia, the AUSTRAC has reemphasized that firms must apply enhanced customer due diligence (ECDD) in high-risk situations. In the EU, MiFID II mandates that all pre-, at-, and post-trade data (including voice and text communications) must be automatically linked for trade reconstruction within 72 hours of the request. In the U.S, several governmental organizations such as the CFTC, DOJ, FBI, IRS, FINRA, FTC and SEC are focused on combating financial crime.

Adoption of multitiered risk-based approach

To protect against digital crime, financial institutions are adopting a customer-centric and segmented risk-based approach. This approach assesses the users' digital actions across multiple tiers including (1) access endpoint (browsing devices and application used), (2) navigation, (3) channel and cross-channel, and (4) association focus.

Tier 1 helps secure the user's access endpoint against ransomware, spyware, computer viruses, etc. Tier 2 helps identify conspicuous suspicious transactions, or malware-induced actions such as uncharacteristic navigation patterns or unusually rapid navigation. Tier 3 analyzes the account or user-centric behavior for individual channels, cross-channels and cross-product behavior of users and accounts. Finally, Tier 4 helps to analyze transaction patterns to establish links between the individual or organization and accounts to discover criminal networks.

Increase in demand for holistic trade surveillance solutions

To effectively combat trade/market manipulation and to comply with regulatory expectations, financial institutions have begun leveraging holistic trade surveillance solutions. These solutions provide an integrated approach. They bring together market, trade, client/

trader/broker, written and voice communication, and many other data points to deliver a unified cross-market/cross-asset picture. Solutions can speedily correlate and analyze data from several disparate sources including videos, emails, chat and text messages, user/access activity logs, security logs, transactional data, and social media. Utilizing these capabilities, solutions can help expose connections between events, trades and communications.

Growth in forward-looking FCRM investments

Financial institutions are making FCRM related investments with an eye on the future. For example, they are (a) investing in integrated and advanced FCRM solutions (that leverage real-time CEP, stream analytics, AI/ML, and other advanced technologies to uncover crimes across digital channels); (b) partnering with fintechs and regtechs for FCRM solutions; and (c) forming consortiums to share relevant data and insights on financial crime.

Trend 3: Mitigating financial risks of climate change

Climate change has become a global challenge with social, political and economic implications to the extent that it was ranked amongst the top five risks as per a World Economic Forum survey. Climate change-related calamities — such as rising global temperatures and sea levels, wildfires, droughts, hurricanes — have had disastrous impacts. For example, 2019 witnessed wildfires in the U.S and Australia, and storms in Japan and the Bahamas.

According to the World Economic Forum, natural calamities caused global economic stress and damage worth US$165 billion in 2018. As per estimates, global warming extracts an economic cost of around US$250 billion per year from the U.S alone. Climate risk exposure has an impact on interest payments as well — over the previous 10 years, developing countries have spent an additional US$40 billion in interest payment on their debt.

Risks to financial institutions

For financial institutions, climate change creates significant financial and non-financial risks including operational, credit, market, legal and reputational risks. It causes risks in the mortgage, lending and insurance businesses, and investments and derivatives portfolio to rise. The 2019 bankruptcy of PG&E, California's biggest utility firm, following the wildfires, highlights the increased credit risks for banks from climate change.

Broadly, there are two categories of risks that financial institutions face from climate change: physical and transition.

Physical risks arise from the physical effects of frequent climate-related events such as floods, storms, droughts and wildfires. These risks result in a heightened risk of default on loan portfolios and a decline in asset values. For example, financial institutions with mortgage portfolios exposed to coastal areas may witness increased credit risk and a decline in collateral value when rising sea levels and floods damage property and result in falling property prices.

Transition risk is related to the shift toward a low-carbon economy to mitigate climate change risks. Such transition may involve policy, regulatory, market and technology changes which could create financial risks for institutions. For example, consider the policy changes to reduce dependence on fossil fuel through energy taxes, new carbon prices, or emission rules. Such policy changes would adversely affect oil, coal and gas producers' businesses. Financial institutions with exposure to such producers or to carbon-intensive industries like the power generation and mining industries, may witness rising levels of non-performing loans. Asset values, such as of stakes in coal-based power plants, could drop. Equity markets may shake-up, for example, through the reduction in fossil fuel related export value.

Increased regulatory and supervisory focus on climate change risks

Regulators and central banks around the world have started focusing on climate change-related financial risks. Here are few instances of how these bodies are taking steps to tackle climate change risks.

Global regulatory bodies

The Financial Stability Board has instituted the "Task Force on Climate-related Financial Disclosures" to recommend institutions to disclose uniform, clear and comparable information on the risks and opportunities that climate change presents to their respective businesses.

Federal regulatory bodies

The Commodity Futures Trading Commission formed a 35-member panel to focus on the physical and transition risks emanating from climate change, and its financial impact on institutions.

The Prudential Regulatory Authority and the Financial Conduct Authority created the Climate Financial Risk Forum (CFRF) that enables financial institutions in the U.K to share best practices and build intellectual capacity on climate change-related financial risks management.

In February 2020, the Australian Prudential Regulation Authority announced that it plans to implement mandatory climate change-related stress tests for banks, insurers and the pension fund industry. Banks will need to assess risks on their business models and loan books under several climate scenarios.

Central banks

The People's Bank of China has undertaken several steps to encourage green financial development. It has included green finance in its macro-prudential assessment system that offers positive incentives for Chinese commercial banks to increase green deposits and green credit stock.

Climate change risk management considerations for financial institutions

Financial institutions are increasingly expected to focus on integrating climate change risks with their FRM framework, evolve their scenario analysis capabilities, and make strategic calls to mitigate climate change related financial risks.

1. Risk integration

- Treating climate change risks as financial risk, and integrating them into the firm's FRM framework
- Understanding the potential impacts of physical and transition risks of climate change on customers, counterparties, and the businesses they invest in
- Integrating climate change risks with the underwriting and credit review processes

2. Scenario analysis

- Leveraging robust scenario analysis tools and techniques
- Considering both physical and transition risk scenarios
- Enhancing the existing stress testing and scenario analysis frameworks in order to accommodate the peculiar nature of climate change scenarios

3. Strategy

- Adopting long-term and firm-wide approaches
- Strategically focusing on risk management, opportunities exploitation, and technology and data aspects
- Proactively collaborating with regulators, central banks and other key external stakeholders to influence regulatory and monetary policy changes

Measures taken by financial institutions to manage climate change risks

Many financial institutions have realized the importance of protecting themselves against the financial risks caused by climate change and have begun taking steps to mitigate them. Here are few examples.

In September 2019, the UN and several prominent banks unveiled the Principles for Responsible Banking. 130 banks together holding US$47 trillion in assets have signed up. Through the principles, financial institutions have promised to align their businesses with the Sustainable Development Goals (SDGs) and the goals of the Paris Agreement on climate change.

Over 50 financial institutions have committed to reduce their greenhouse gas (GHG) discharges in line with the Paris Agreement, through the Science-Based Targets initiative. ING Group, HSBC, Societe Generale, Credit Agricole, and AXA Group are among these financial institutions.

In 2019, Citigroup established a working group to integrate the climate change related issues with its risk management controls. It also released its first climate report in line with the TCFD guidelines. The bank has partnered with its peers to develop pilot models to assess how climate change-related scenarios may impact loan portfolio performance.

The European Investment Bank plans to stop financing fossil fuel projects from the end of 2021 in its efforts to mitigate climate change risks.

The Royal Bank of Scotland has said that it will reduce to zero the net greenhouse-gas (GHG) emissions of its operations in 2020. The bank aims to become "climate positive," to capture more carbon than it emits, by 2025.

Commonwealth Bank of Australia and Westpac are analyzing climate change-related scenarios on their portfolios. ANZ also plans to focus on climate-related risk governance and stress testing of its specific portfolios.

DIGITAL TO TRANSFORM THE RISK AND COMPLIANCE FUNCTION

Until recently, the majority of a financial institution's digitization efforts have been focused on their customer-facing business functions. Institutions have however been slow to adopt these new-age digital technologies in their risk and compliance functions because of the significance that these functions carry. This is gradually changing, however.

Recently, an increasing number of financial institutions have begun adopting advanced technologies — such as cloud, artificial intelligence, and machine learning — to enhance transparency, improve decision-making and reduce the cost of their risk and compliance management operations. Several use-cases for digital technology adoption — such as in GRC, credit risk management, and financial crime risk management — have already been executed by institutions. Many more are in the evaluation stage.

Trend 4: Rising digital adoption in GRC

As businesses become increasingly complex and technology advances, organizations' governance, risk management and compliance (GRC) applications have rapidly evolved. The global enterprise GRC or eGRC market is estimated to reach US$60.8 billion by 2025, from US$32.3 billion in 2020, growing at a CAGR of 13.4%, as per a MarketsandMarkets report. The financial services industry contributes the largest share to this market.

Digital adoption is expected to be a key driver of the eGRC market growth. Institutions are increasingly adopting digital technologies in their GRC function to effectively comply with regulatory mandates, holistically manage risks, and ensure sound governance. These digital technologies mostly include advanced and predictive analytics, big data, cloud, artificial intelligence (AI), machine learning (ML), natural language processing (NLP), robotic process automation (RPA), and blockchain.

Benefits of digital GRC to financial institutions

Digital technologies bring multiple benefits to financial institutions. They help save costs, improve productivity and increase efficiency, while maintaining the trust quotient. A look at how each technology positively impacts eGRC includes these issues.

The cloud model helps reduce the total cost of ownership (TCO), avoid large upfront investments, and reduce capital expenditure on IT infrastructure. This flexible model helps institutions scale quickly to respond to their ever-evolving GRC requirements. Firms don't need to engage in a prolonged IT development lifecycle. Instead, the cloud providers supervise software upgrades and security updates. Cloud also enables continuous system availability and provides robust disaster recovery capabilities. For example, MetricStream's GRC Cloud solution, which is built on state-of-the-art containerization and virtualization technologies, enables firms to quickly deploy GRC apps — for audit management, risk management, and corporate and regulatory compliance — in the cloud. The solution provides optimal security, reliability and scalability, and require substantially less investment than does traditional on-premises infrastructure.

Many machine learning techniques such as Markov Chain Modeling, Random Forest, Deep Learning are being used in digital GRC. These help financial institutions (a) optimize enterprise risk or regulatory models and parameters; (b) automatically analyze and map regulatory requirements to business processes and controls; (c) identify emerging risk patterns including cybersecurity and AML typologies or the techniques used to launder money; (d) support sophisticated risk scoring; and (e) auto-suppress false positives. Similarly, AI-backed NLP capabilities help institutions (a) generate applicable requirements from the new regulations, (b) identify suspect communications or transactions based on free-form text, and (c) perform extended due diligence via data correlation of various unstructured sources.

RPA enhances the productivity and effectiveness of the GRC function. For example, RPA and AI are being used to automate the testing of controls, speed up execution, reduce operating costs, and ensure that all controls have been tested. The technology also monitors the controls, collects GRC data from multiple sources, automates manual controls, and executes several GRC activities.

Blockchain's immutability characteristic helps establish proof of process and chain of trust. This makes it apt for GRC activities including counterparty risk management, risk underwriting, and policy and regulatory change management.

Trend 5: Uptake in integrated digital credit risk management solution is rising

Over the past few years, the complexities of the credit environment have increased manifold. Regulatory expectations from financial institutions have intensified too. Institutions need to comply with several credit risk management related regulatory requirements and standards such as Basel III, CECL and IFRS 9.

Most financial institutions' legacy credit risk management systems have not kept pace with these developments. These systems comprise assortments of siloed credit scoring and decisioning that are unable to provide a holistic view to the credit underwriter — regarding the risks involved, product pricing, customer lifetime value and other key factors. These legacy systems require manual intervention, involve huge maintenance cost and are difficult to integrate with the newer digital channels and systems. Critical situations such as the current COVID-19 outbreak have further exposed the weaknesses of such systems.

Owing to these shortcomings, financial institutions have been unable to optimally manage their credit risks. As a result, they are facing significant financial losses as well as the regulators' ire. As per the 10th annual EY/IIF Global Bank Risk Management survey, one of the major risks to manage in the next decade will be meeting customer demands for a lifetime offering. To mitigate this risk, around 60% of CROs realize that integrated risk platforms need to be implemented.

An increasing number of financial institutions have begun adopting integrated digital credit risk management solutions. For example, Next Commercial Bank (NCB), Taiwan's first digital bank, has implemented Kamakura Corporation's suite of integrated risk management solutions. By adopting these integrated solutions, financial institutions expect to lower their TCO, improve risk management and accelerate decision making.

Features of an integrated digital credit risk management solution

Following are some of the main features provided by integrated digital credit risk management solutions:

- Offers seamless integration with other internal systems such as core banking, CIS, CRM, loan origination, rating models, portfolio management, collateral management, etc.
- Enables a 360-degree view and the generation of holistic risk metrics by ingesting data from multiple internal and external sources across business lines and asset classes.
- Supports (a) sophisticated pre-screening and prospecting, and (b) enhanced portfolio management and recovery.
- Empowers data management and governance — such as reference data management, automated data quality review, data access and security, etc.
- Offers sophisticated analytics capabilities that enable (a) real-time risk scoring and credit underwriting, (b) limits monitoring, (c) early warning signals and timely alerts, and (d) advanced reporting and dashboards.
- Leverages cognitive analytics and artificial intelligence (AI) capabilities — including ML, NLP and RPA technologies — in relevant credit risk management processes such as loan application processing, credit scoring and decisioning, loan pricing, and credit default prediction.

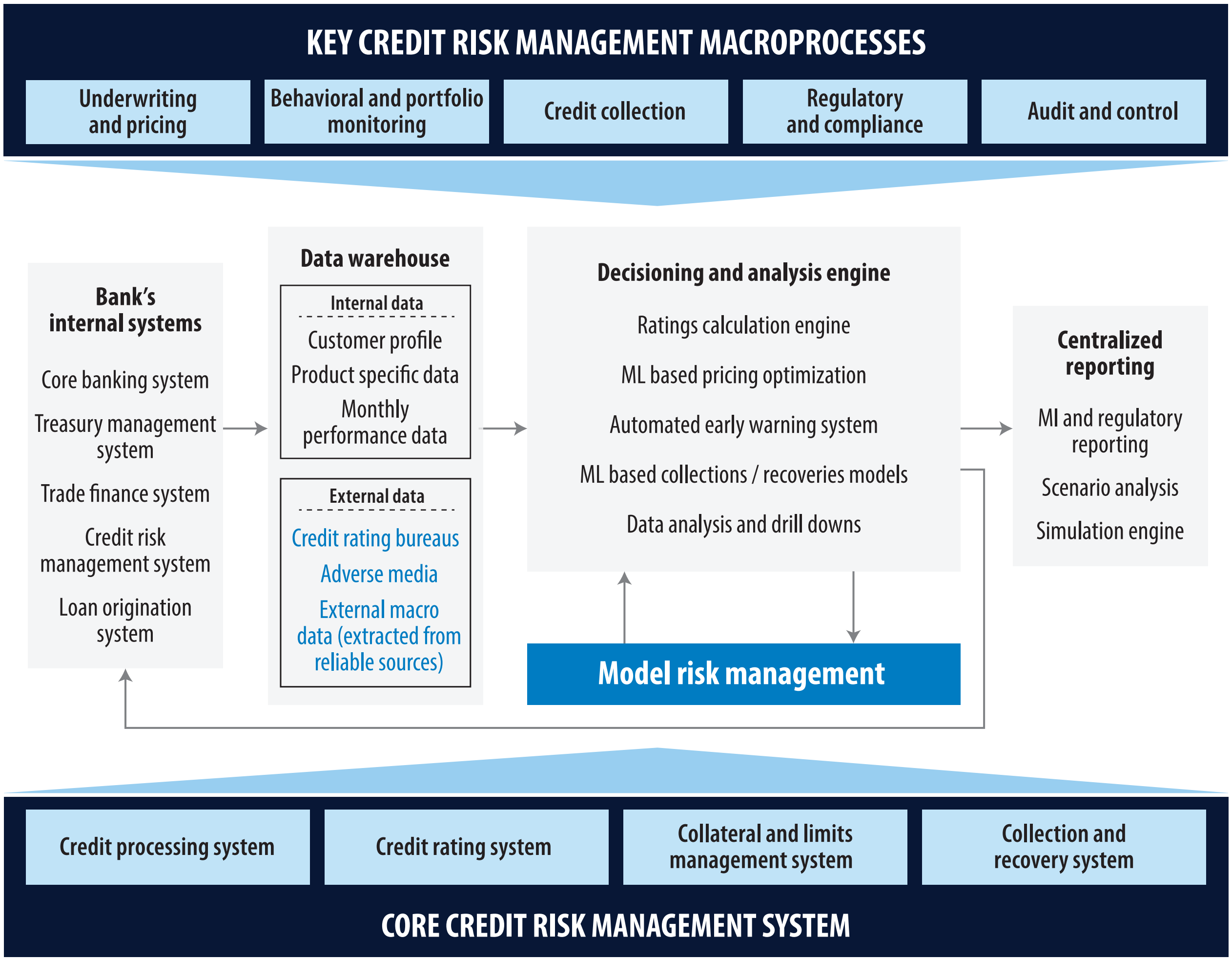
Examples of advanced analytics and AI/ML adoption in credit risk management

Zest Finance and Experian have implemented AI-powered underwriting solutions on alternate data sources to assess borrowers' lending ability.

Lenddo profits rose nearly 54% after it used a combination of traditional and alternate data-based models on risky unbanked population.

JPMorgan Chase's COiN, a contract intelligence platform, uses ML to review 12,000 annual commercial-credit-agreements in seconds, that would have otherwise taken the bank's staff ~360,000 hours a year to analyze.

Figure 1. Illustrative integrated credit risk management solution


KEY CREDIT RISK MANAGEMENT MACROPROCESSES
Underwriting and pricing
Behavioral and portfolio monitoring
Credit collection
Regulatory and compliance
Audit and control
Bank's internal systems
Core banking system
Treasury management system
Trade finance system
Credit risk management system
Loan origination system
Data warehouse
Internal data
Customer profile
Product specific data
Monthly performance data
External data
Credit rating bureaus
Adverse media
External macro data (extracted from reliable sources)
Decisioning and analysis engine
Ratings calculation engine
ML based pricing optimization
Automated early warning system
ML based collections / recoveries models
Data analysis and drill downs
Model risk management
Centralized reporting
MI and regulatory reporting
Scenario analysis
Simulation engine
Credit processing system
Credit rating system
Collateral and limits management system
Collection and recovery system
CORE CREDIT RISK MANAGEMENT SYSTEM

Source: Infosys

Trend 6: Increasing adoption of AI capabilities to fight financial crime

Financial institutions have realized that their incumbent legacy FCRM solutions cannot support their needs. These rigid rules-based systems: (a) lack predictive abilities; (b) are unable to manage the volume, variety and velocity of today's threats; (c) are error-prone and yield high number of false positives; (d) have inefficient workflow and require significant manual intervention; and (e) are unable to keep pace with enhanced regulatory expectations.

To overcome these challenges, financial institutions have begun adopting new-age anti-financial crime (AFC) solutions that leverage AI capabilities including ML, RPA and NLP. Some of the leading AFC solution vendors are also investing in deep learning and advanced Explainable AI (XAI) technologies to allow the results from the decision engines to be understandable to experts.

AI adoption use cases

Here are some of the use cases of AI that financial institutions have implemented or plan to implement.

AI and ML adoption in FCRM

	Domain	Use case
1	KYC	• Remote identity pre-checks • Customer onboarding • Real-time transaction-based KYC anomaly detection • Sophisticated link analysis • Intelligent customer segmentation • Automatic KYC scoring (by scanning social media, police registers, etc.)
2	AML	• Screening • Holistic transaction monitoring and analysis • Generating insights on new money laundering typologies • Investigation queues prioritization (using sophisticated AML risk scoring) • Adaptive real-time monitoring of high-risk entities (against OFAC, SDN, etc.) • Enabling true identity-matching • UBOs and PEPs identification • False positives reduction
3	Fraud management	• Fraud detection • Customer screening • Transaction monitoring • Alert investigation • Link analysis • Customer segmentation • Sophisticated fraud risk scoring • False positives reduction
4	Trade and market surveillance	• Holistic surveillance (by leveraging NLP to examine both the traders' transactions and communications) • Alert scoring, forecasting and threshold analysis • Link analysis and cross-asset linked alerting • Spoofing detection • Surveillance quality control • Dynamic maintenance of the traders' profile • In the market surveillance programs of exchanges/regulators • Predictive scoring
5	Rogue employee detection	• Monitoring of employees' behavioral profile patterns, communication and transactions to unearth collusion/fraud

RPA adoption in FCRM

	Domain	Use case
1	KYC	• Customer data setup and consolidation • Customer screening (vis-à-vis OFAC, PEP, negative news, etc.) • Customer info extraction, validation and compilation • KYC data remediation • Capture results from customer screening • Flag missing/mismatched/outdated info
2	AML	• Automated alert investigation • Enable efficiency gains in alert/case management • Customer info extraction, consolidation, validation and compilation • Document analysis
3	Trade surveillance	• Tasks and workflow automation • Automatic order book reconstruction, trade reconstruction and market replay

Examples of AI adoption in FCRM

HSBC has partnered with Ayasdi, Inc. to automate its regulatory compliance processes. HSBC employs Ayasdi's AI-based solution to automate its AML investigation processes.

Hong Kong Exchanges and Clearing Limited has implemented, across its equity market, Nasdaq SMARTS Market Surveillance's ML-based solution and the participant-relationship discovery technology.

Danske Bank is using Think Big Analytics' (a Teradata firm) AI-driven fraud detection platform. The solution's machine learning capability evaluates thousands of probable features. Additionally, it scores millions of online transactions in real-time, to offer actionable insights on illegal transactions.

Nasdaq has utilized machine learning to score and rank customer alerts that are generated by its trade surveillance solutions.

Standard Bank, Africa's largest bank, has adopted WorkFusion's RPA- and AI-based solution to reduce the time taken for client onboarding and KYC from 20 days to just five minutes.

Japan Exchange Regulation (JPX-R) and Tokyo Stock Exchange (TSE) are utilizing an AI-based solution for their market surveillance operations. The solution assists surveillance personnel in conducting preliminary investigations quicker. By leveraging its machine learning capabilities, the solution can learn the earlier operations related to evaluation of irregularities performed by the surveillance personnel.

Trend 7: Leverage cloud-based managed service offerings to combat financial crime risk

Building an anti-financial crime (AFC) infrastructure in-house is expensive. The costs include server maintenance (for the CPU-intensive FCRM processes), licensing, security patching, software upgrades and regular updates to watchlists. Small and medium financial institutions find it uneconomical to build robust AFC solutions. Many large financial institutions also want to avoid the complexities involved in managing in-house AFC platforms.

Cloud-based models and an increasing number of partnerships between product companies and system integrators to provide software-as-a-service (SaaS) AFC offerings are making advanced AFC solutions affordable at scale for financial institutions. For example, Infosys and NICE Actimize partnered to provide end-to-end AFC solutions, where Infosys offers its delivery capabilities and enables NICE Actimize's end-to-end AFC solutions via cloud or in an on-premises environment.

SaaS-based AFC offerings are a relatively new area for compliance solutions and help deliver scalable, reliable and cost-effective solutions. Financial institutions can better manage IT costs and lower their total cost of ownership vis-à-vis change management, implementation, onboarding, maintenance and support. They also helped ensure autonomous and adaptive delivery, as the latest versions of AFC software are automatically deployed at the flexible scale of cloud. The SaaS model aligns well with a financial institution's APIfication strategy to adopt open banking. Most often, the system integrator responsible for moving infrastructure from legacy to the cloud enables a self-updating agile technology infrastructure that prevents the accumulation of technical debt.

These SaaS-based AFC offerings now have been expanded to create end-to-end business outcome-based services for banks. They bring in integrated technology and business process management capabilities, packaged and offered as a subscription model. Here are a few examples of cloud-based managed services in the AFC domain:

	Service category	Description of managed services support to various subcategories
1	**KYC-as-a-Service**	• Supports client identity and verification, and KYC screening and monitoring to enable quick on-boarding, and remediation and refresh of KYC policies • Enables a comprehensive single-view-of-the-customer to support identity verification, and KYC screening • Streamlines the due diligence documentation workflow, and the KYC compliance processes • Integrates legal entity information (LEI) from reliable sources across countries and languages • Provides a central KYC data pool that can be shared across financial institutions, thereby enabling (a) economies of scale and cost efficiency, and (b) a transparent and collaborative KYC data approach amongst industry participants
2	**AML-as-a-Service**	• Enables customer due diligence (CDD) including customer risk rating, sanctions and PEP screening, enhanced due diligence (EDD), and re-screening of high-risk customers • Supports ongoing real-time AML transaction monitoring, and the associated processes such as transactions profiling, suspicious activity review, alert/case investigation workflow • Provides access to up-to-date and comprehensive AML databases including sanctions and PEP lists • Assists timely reporting such as suspicious activity report (SAR) filing, MIS reporting, etc.
3	**Fraud-Prevention-as-a-Service**	• Uses a multitiered risk-based approach for fraud prevention • Supports all digital channels (including mobile and web applications) • Enables cognitive solution to combat various forms of fraud including phishing, malware, account takeover, social engineering scams, man-in-the-middle fraud, etc.

CONTINUED FOCUS ON REGULATORY COMPLIANCE

The implementation dates of several key regulatory mandates such as the LIBOR transition and FRTB are on the horizon. Financial institutions have been working with full intensity to make the required business, IT and operational changes to be compliant. They are also focusing on bolstering their regulatory reporting capabilities — in order to keep pace with the enhanced regulatory scrutiny of their financial and nonfinancial risks.

Trend 8: LIBOR transition remains a key priority

For years, the London Interbank Offered Rates (LIBOR) had been the reigning interbank benchmark rate used by global banks. Over US$400 trillion of assets (including derivatives, bonds, mortgages and other loans) referenced the LIBOR as of mid-2018.

Yet, after global banks were alleged to have indulged in manipulation, regulatory agencies decided to replace the LIBOR with more sustainable alternative reference rates (ARRs) in their local currency. These ARRs include SOFR (U.S.), SONIA (U.K), ESTER (Euro Area), SARON (Switzerland), and TONIA (Japan).

The U.K.'s Financial Conduct Authority (FCA) has decided that it won't compel banks to submit LIBOR quotations after 2021. As per the FCA, BoE and Sterling Risk-Free Reference Rates Working Group, the COVID-19 crisis will not have an impact on the LIBOR phase out date. However, the pandemic may affect interim milestones in the LIBOR transition.

Impact of the transition

The LIBOR transition is anticipated to be amongst the most substantial changes in the financial services industry, affecting a wide range of products and market participants. The transition will likely impact nearly all business units and functions of the concerned financial institutions — including counterparty and customer management, product strategy, contracts, financial processes, risk models, and IT systems. Institutions would face significant operational, financial, legal and reputational risks.

Action for financial institutions

Given its huge impact, the LIBOR transition has become a key priority for all concerned financial institutions. Here are the activities that firms have been engaged in to be prepared:

Impact assessment

- Identifying LIBOR exposures
- Evaluating the financial and nonfinancial impact of the transition on the balance sheet, accounting and tax treatment, ALM, contracts, currencies, jurisdictions, clients, products, processes, infrastructure and IT systems

Risk assessment

- LoBs level detailed risk assessments — vis-à-vis products, clients, operations, processes and IT
- Ascertaining the amendments required to the risk methodology and valuation

Contracts review

- Analyzing the need to update standardized contracts — for example contracts related to fallback clause — and to design new business contracts

Transition planning

- Vis-à-vis operational processes, risk models update/development, controls updates, and products enhancements (cash, derivatives, linked to risk-free reference rates (RFR), with fallback provisions, etc.)
- Create a transition roadmap that includes back-book and legacy trades

Planning for IT changes

- **Data management systems:** Sourcing data including market data feed and vendor data for new products, validation, and system enhancements
- **Risk management systems:** Risk modeling systems
- **Trading systems:** Retooling and reconfiguration of platforms to allow trade pricing, capture and execution of ARR-referencing products
- **Post-trade processing systems:** Back-office systems update to support booking/processing/valuation of ARR-referencing products
- **Treasury and ALM systems:** Improving ALM processes including cash-flow forecasting and balance sheet funding, and ARR-referencing products
- **Reporting systems:** Enhancing MIS and dashboards

Regulatory focus

Given the magnitude and complexity of changes involved in the LIBOR transition, regulators around the world including the FSB, SEC, NYDFS, ECB and FCA, have been monitoring the progress that financial institutions are making. This regulatory scrutiny would likely intensify closer to the 2021 deadline.

Trend 9: Continued focus on FRTB implementation

In January 2016, the BCBS published new rules pertaining to the market risk framework for capital requirements, known as Fundamental Review of the Trading Book (FRTB). These rules address Basel 2.5 vulnerabilities related to internal risk transfers, under-capitalization of trading books, and capital arbitrage between trading and banking books.

Through FRTB, the BCBS intends to (a) create a distinct boundary between the trading and banking books, and minimize the incentives for capital arbitrage, (b) strengthen market risk standards and provide a consistent framework for financial institutions to capitalize their trading activities, and (c) ensure that both the internal model approach (FRTB-IMA) and the standardized approach (FRTB-SA) to market risk can offer reliable capital outcomes.

COVID-19 has forced BCBS to defer the implementation of Basel III mandates, including those related to FRTB, from January 1, 2022 to January 1, 2023. This extension allows financial institutions and supervisors to enhance their operational capacity to respond to the ongoing pandemic.

The global FRTB rules need to be adapted to each country's local reporting standards. This is a challenging task. It is highly likely that not all the countries will be able to adhere to the BCBS deadline.

FRTB implementation challenges

FRTB creates massive implementation complexities and cost requirements for the banking sector. Investment banks and Tier 1 and Tier 2 universal banks with substantial capital markets business are especially impacted. The new rules are expected to increase the amount of risk-weighted capital that banks need to hold in reserve. To comply with the FRTB requirements, financial institutions must make changes to their front- and back-office functions — including infrastructure, IT, risk, operations, data sourcing, data management, and quantitative modeling.

FRTB implementation focus areas of financial institutions

The following are some of the main activities that financial institutions are focusing on:

1. Business strategy

- The financial implications of FRTB are compelling financial institutions to consider whether and how to reduce their trading activities, or to exit certain business lines.
- Owing to the complexities involved in implementing the internal model approach (FRTB-IMA), many small-sized banks (Tier 2 and below) may adopt the standardized approach (FRTB-SA).

2. P&L attribution test

- Financial institutions are analyzing their sensitivities to instrument prices and pricing models that are crucial for P&L reporting and market risk management.
- Firms are working to ensure consistency between the calculations utilized for computing sensitivities and the valuation models used by front-office for trading purposes.

[Note: The P&L attribution test helps assess the efficiency of a financial institution's internal models and checks to see if relevant risks that impact the portfolio are captured. In order to leverage FRTB-IMA, each trading desk in the firm must individually pass this test.]

3. FRTB Risk Factor Eligibility Test (RFET)

- Financial institutions are analyzing their existing risk factor analysis (RFA) and liquidity horizon management aspects. The aim is to strengthen the processes related to identifying modellable risk factors (MRFs) and non-modellable risk factors (NMRFs) for inclusion in internal models.

[Note: To pass the RFET, a risk factor utilized by a financial institution in its internal model must fulfil certain criteria on a quarterly basis. Otherwise, it would be classified as NMRF. Under FRTB, this means that

the risk factor lacks ample price data to allow internal modelling. NMRFs lead to higher capital charges for financial institutions.]

4. Revised standardized approach (SA) for sensitivities-based method

- Firms are strategizing to fulfil the regulatory expectations under FRTB's new sensitivity factor norms such as identification of risk factors, estimating net sensitivities by risk factor, and calculating weighted sensitivities.

[Note: The sensitivities of financial instruments to certain risk factors are utilized for computing the delta/vega/curvature risk capital requirements.]

5. Data requirements and risk measures

- Effective data management and access to high-quality data, such as on observation, across asset classes and trade activity are key to successfully implement FRTB. Hence, institutions have been (a) analyzing the data requirements for internal data, third party data, and global market data pools; (b) designing market data sourcing strategy; and (c) ascertaining the changes required for IT and data infrastructure vis-à-vis data sources standardization, data lake, computational capacity for FRTB calculations, etc.

Trend 10: Regulatory reporting solution market is growing rapidly

The global regulatory reporting solutions market is estimated to grow at a five-year CAGR of 18.7% between 2020 and 2025, with the Asia-Pacific region leading the market share. In the Asia-Pacific region, global regulatory mandates such as the Basel III net-stable-funding-ratio (NSFR) are being implemented. Regional regulators also are intensifying their regulatory reporting requirements.

Factors that are leading to the rapid growth in the regulatory reporting solutions market include the following:

Heightened expectations from the regulators

- The reporting scope, complexity, volume, frequency, and required levels of disclosures and details have intensified. There is an increase in ad-hoc reporting requirements. Also, regulators expect institutions' reports to be accurate, complete, traceable, auditable, and delivered on time.
- Many financial institutions need to file hundreds of reports with numerous regulatory agencies. For instance, for the U.S. Federal Reserve alone, concerned firms need to generate several reports related to stress testing, FFIEC 101, call reports, etc.
- New reporting obligations, such as those related to CCAR, Basel and FR Y-14, require financial institutions to gather, validate, reconcile and synthesize data from across the various departments (such as accounting, finance, risk, and business segments) and systems (such as planning, front office, accounting, risk, capital management, liquidity and treasury management).

Note: Amidst the COVID-19 crisis, regulators such as the U.S. SEC, the Federal Reserve, EBA, APRA, RBA and ABS, have provided grace periods to financial institutions to file certain reports such as the quarterly reports, FR Y-9C, FR Y-11, call reports, Pillar-3-disclosures, etc. Regulators also have deferred the announcement of several new reporting obligations.

Multiple reporting standards and formats

- The number of regulatory reporting standards and formats have risen manifold and lack international compatibility and consistency. For example, reporting mandates such as MiFID II/ MiFIR, FATCA, EMIR, COREP, FINREP require financial institutions to submit reports utilizing different standards and formats (such as XBRL, XML, CSV, FTP, MS Excel, FpML, ASCII, etc.).

Suboptimal legacy reporting systems

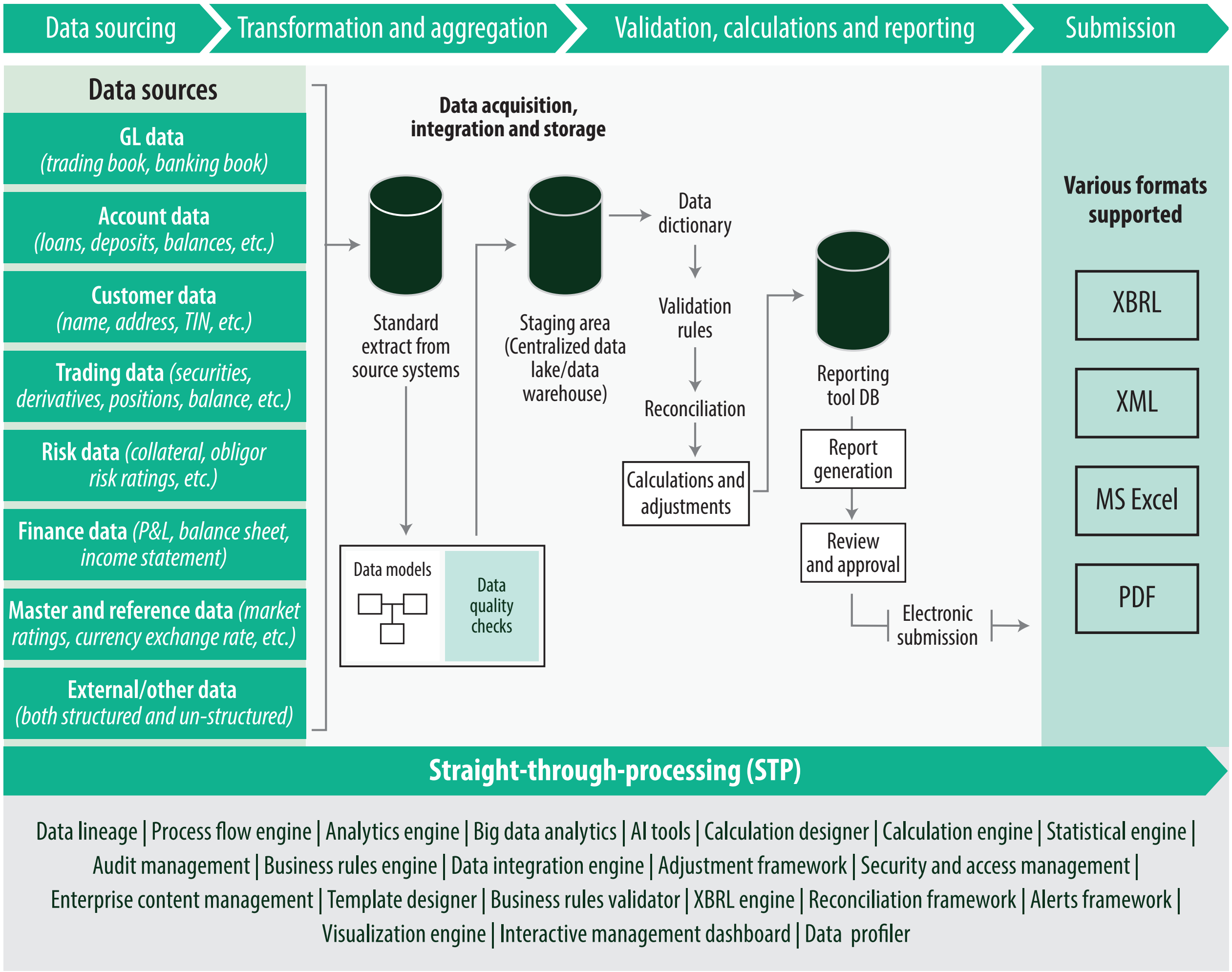
- Institutions lack end-to-end data management and reporting capabilities. Their existing reporting solution workflow requires significant manual interventions — vis-a-vis data sourcing, aggregation, cleansing, classification, adjustments, reconciliations and submission. This has led to higher manpower requirement and increase in costs and reporting errors.
- Supporting tools such as those used for dashboards are not being adopted. Consequently, financial institutions are forced to rely on tactical tools such as end-user computing and spreadsheets.

Given the aforementioned factors, financial institutions have begun adopting integrated end-to-end reporting platforms to manage their regulatory reporting needs. These platforms are expected to have the following features:

- Seamlessly integrates with and processes data from various IT systems including risk, finance, business lines, regulatory, CIS, other core systems, and calculation engines
- Leverages centralized data warehouses/lake to offer a single source of truth (SSOT)
- Enables automated end-to-end regulatory reporting processes encompassing data acquisition, reconciliation, aggregation and standardization; calculation and classification; and report generation, review, approval and submission
- Provides a frictionless user interface and reporting tools such as inbuilt reporting templates, template designer, interactive dashboards and drill-down capabilities, and various reporting formats
- Offers scalable and modular architecture and integrated reporting governance

Here is an illustrative functional architecture of an integrated reporting platform.

Figure 2. Integrated end-to-end reporting platform: Illustrative functional architecture


Data sourcing
Transformation and aggregation
Validation, calculations and reporting
Submission
Data sources
GL data (trading book, banking book)
Account data (loans, deposits, balances, etc.)
Customer data (name, address, TIN, etc.)
Trading data (securities, derivatives, positions, balance, etc.)
Risk data (collateral, obligor risk ratings, etc.)
Finance data (P&L, balance sheet, income statement)
Master and reference data (market ratings, currency exchange rate, etc.)
External/other data (both structured and un-structured)
Data acquisition, integration and storage
Standard extract from source systems
Staging area (Centralized data lake/data warehouse)
Data dictionary
Validation rules
Reconciliation
Calculations and adjustments
Data models
Data quality checks
Reporting tool DB
Report generation
Review and approval
Electronic submission
Various formats supported
XBRL
XML
MS Excel
PDF
Straight-through-processing (STP)
Data lineage | Process flow engine | Analytics engine | Big data analytics | AI tools | Calculation designer | Calculation engine | Statistical engine |
Audit management | Business rules engine | Data integration engine | Adjustment framework | Security and access management |
Enterprise content management | Template designer | Business rules validator | XBRL engine | Reconciliation framework | Alerts framework |
Visualization engine | Interactive management dashboard | Data profiler

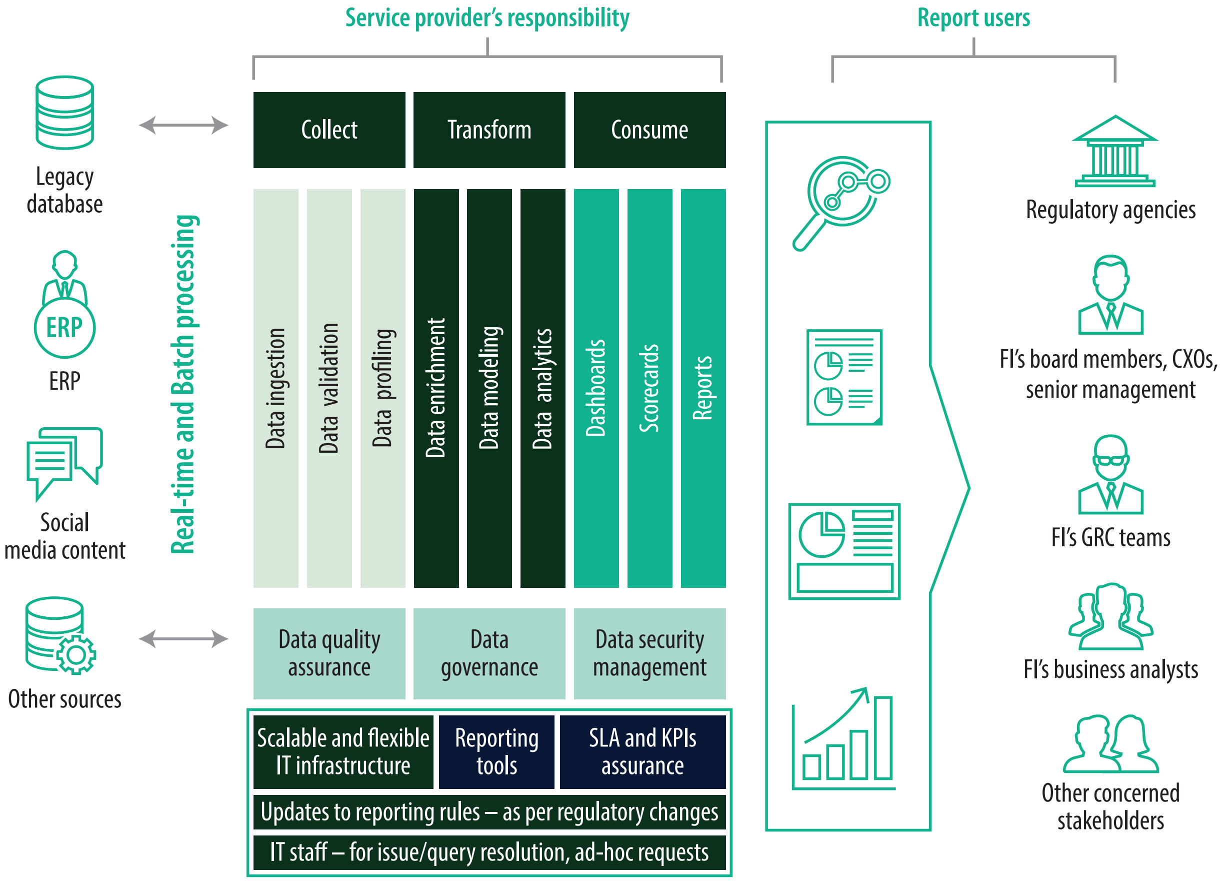
Source: Infosys

Several financial institutions — especially the small and medium-sized ones — are adopting a hosted cloud-based regulatory reporting as a service (RRaaS) model. According to Wolters Kluwer, nearly 30% of regional financial institutions in theAsia-Pacific region plan to use cloud for their regulatory reporting.

The RRaaS model involves the outsourcing (or co-sourcing) of regulatory reporting obligations. The financial institution's end-to-end reporting responsibilities and processes are centralized with a service provider, which updates and maintains the regulatory reporting IT infrastructure as well.

The RRaaS model can help financial institutions revamp their reporting capabilities. The model provides institutions with efficiency gains and cost savings and enhances their reporting flexibility and scalability. It mitigates the challenges associated with building, managing, enhancing and monitoring the regulatory reporting infrastructure. For an illustrative RRaaS model see Figure 3, Illustrative RRaaS model.

Figure 3. Illustrative RRaaS model



Source: Infosys

Examples of RRaaS offerings

Suade Labs provides Regulation-as-a-Service (RaaS) via a software platform. The platform enables financial institutions to process huge volumes of data to generate required calculations, regulatory data, and reports. The platform is fast — it takes four minutes to generate a report on 56 million rows of data.

Finastra's RRaaS solution is hosted in its private cloud. The solution gathers and inspects transaction information from banks' own or third-party system. It allows banks to effectively handle new and changing reporting requirements such as those related to SFTR, MiFID II and EMIR.

Acronyms

6AMLD – Sixth Anti-Money Laundering Directive

ABS – Australian-Bureau of Statistics

AFC – Anti-Financial Crime

AI – Artificial Intelligence

ALM – Asset and Liability Management

AML – Anti-Money Laundering

API – Application Programming Interface

APRA – Australian Prudential Regulation Authority

ARRs – Alternative Reference Rates

BCBS – Basel Committee on Banking Supervision

BCDR – Business Continuity and Disaster Recovery

BCM – Business Continuity Management

BCP/DR – Business Continuity Planning and Disaster Recovery

BIS – Bank for International Settlements

CCAR – Comprehensive Capital Analysis and Review

CCP – Central Counterparty

CDC – Centers for Disease Control and Prevention

CECL – Current Expected Credit Loss Accounting Standard

CEP – Complex Event Processing

CFPB – Consumer Financial Protection Bureau

CFRG – Canadian Financial Sector Resiliency Group

CFTC – Commodity Futures Trading Commission

COREP – Common Reporting

COVID – Coronavirus Disease

CRM – Customer Relationship Management

DFAST – Dodd-Frank Act Stress Testing

DOJ – United States Department of Justice

EAD – Exposure at Default

EBA – European Banking Authority

EBRD – European Bank for Reconstruction and Development

ECB – European Central Bank

ECDD – Enhanced Customer Due Diligence

EMIR – European Market Infrastructure Regulation

ESTER – Euro Short-Term Rate

EWS – Early Warning Systems

FASB – Financial Accounting Standards Board

FATCA – Foreign Account Tax Compliance Act

FBI – Federal Bureau of Investigation

FCA – Financial Conduct Authority

FCRM – Financial Crime Risk Management

FFIEC – Federal Financial Institutions Examination Council

FI – Financial Institution

FINRA – Financial Industry Regulatory Authority

FINREP – Financial Reporting

FpML – Financial Products Markup Language

FRTB – Fundamental Review of the Trading Book

FRB – Federal Reserve Board

FSB – Financial Stability Board

FTC – Federal Trade Commission

FTP – File Transfer Protocol

GRC – Governance, Risk Management, and Compliance

G-SIB – Global Systemically Important Bank

IBORs – Interbank Offered Rates

ICR – Intelligent Character Recognition

IFRS – International Financial Reporting Standards

IMA – Internal Models Approach

IOSCO – International Organization of Securities Commissions

IRS – Internal Revenue Service

IT – Information Technology

KYC – Know Your Customer

LGD – Loss Given Default

LIBOR – London Interbank Offered Rate

LOB – Line of Business

MiFID – Markets in Financial Instruments Directive

MiFIR – Markets in Financial Instruments Regulation

ML – Machine Learning

MRFs – Modellable Risk Factors

NGFS – Network of Central Banks and Supervisors for Greening the Financial System

NMRFs – Non-Modellable Risk Factors

NLP – Natural Language Processing

NYDFS – New York State Department of Financial Services

OCR – Optical Character Recognition

OFAC – Office of Foreign Assets Control

ORM –Operational Risk Management

PD – Probability of Default

PEP – Politically Exposed Person

PRA – Prudential Regulatory Authority

RBA – Reserve Bank of Australia

RFET – Risk Factor Eligibility Test

RPA – Robotic Process Automation

RRaaS – Regulatory Reporting as a Service

SA – Standardized Approach

SaaS – Software as a Service

SARON – Swiss Average Rate Overnight

SDN – Specially Designated Nationals

SEC – U.S. Securities and Exchange Commission

SFTR – Securities Financing Transactions Regulation

SOFR – Secured Overnight Financing Rate

SONIA – Sterling Overnight Index Average

STP – Straight Through Processing

TCO – Total Cost of Ownership

TONIA – Tokyo Overnight Average Rate

TPRM – Third Party Risk Management

UBO – Ultimate Beneficial Owner

WEF – World Economic Forum

WFE – World Federation of Exchanges

WHO – World Health Organization

XAI – Explainable AI

XBRL – eXtensible Business Reporting Language

XML – eXtensible Markup Language

References

Trend 1: Strengthen operational resilience with technology

- https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-banking-regulatory-outlook-2020.pdf
- https://www.ey.com/en_in/banking-capital-markets/why-banks-must-view-operational-resilience-as-a-strategic-imperative
- https://www.bis.org/fsi/fsibriefs2.htm
- https://www.corporatecomplianceinsights.com/regulatory-supervision-operational-resilience/
- https://www.globalriskregulator.com/Subjects/Reporting-and-Governance/Preparing-for-a-testing-2020
- https://www.chasecooper.com/uncategorized/operational-resilience-why-scenario-analysis-should-be-an-essential-ingredient
- https://www.finextra.com/newsarticle/35087/lloyds-goes-all-in-on-microsoft-managed-desktop
- https://www.bankofcanada.ca/2018/05/strengthening-cyber-defences/
- https://www.bankofcanada.ca/2019/06/bank-of-canada-announces-partnership-improve-resilience-financial-sector/
- https://www.finextra.com/pressarticle/82668/world-federation-of-exchanges-publishes-update-on-industry-cyber-efforts-during-the-pandemic
- https://www.world-exchanges.org/storage/app/media/cyber-security-in-the-age-of-covid-19-board-003.pdf

Trend 2: The FCRM space is evolving dynamically

- https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf
- https://www.actionfraud.police.uk/covid19
- https://risk.lexisnexis.com/insights-resources/research/true-cost-of-fraud-study-financial-services-and-lending-edition
- https://www.ey.com/en_gl/disrupting-financial-crime
- https://www.infosys.com/industries/financial-services/white-papers/Documents/new-age-efrauds-challenging-fis.pdf
- https://www.finextra.com/blogposting/14485/to-truly-transform-kyc-and-aml-operations-adopt-ai-and-ml
- https://www.infosys.com/industries/financial-services/white-papers/Documents/new-age-electronic-frauds.pdf
- https://www.fiserv.com/en/about-fiserv/the-point/2020-trends-in-fraud-and-financial-crime-risk-management.html
- https://www.riskscreen.com/kyc360/news/another-kind-of-outbreak-covid-19-as-financial-crime-threat/
- https://www.finextra.com/blogposting/17389/key-ingredients-for-implementing-successful-holistic-trade-surveillance
- https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html
- https://www.infosys.com/industries/financial-services/white-papers/Documents/robust-compliance-systems.pdf
- https://www.accountantsdaily.com.au/business/13831-ey-flags-10-banking-risks-to-look-out-for
- https://www.ey.com/en_cy/news/2020-press-releases/01/ey-non-financial-risks-remain-significant-for-banks
- https://rdc.com/kyc-aml/blog/sixth-anti-money-laundering-directive-6amld/
- https://www.austrac.gov.au/business/how-comply-and-report-guidance-and-resources/amlctf-programs/enhanced-customer-due-diligence-ecdd-program

Trend 3: Mitigating financial risks of climate change

- http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf
- https://www.newsweek.com/rising-seas-could-cost-world-14-trillion-year-2100-1006823
- https://www.nytimes.com/2019/01/29/business/pge-bankruptcy.html
- https://www.unenvironment.org/news-and-stories/press-release/130-banks-holding-usd-47-trillion-assets-commit-climate-action-and
- https://www.responsible-investor.com/articles/how-can-financial-institutions-deliver-on-the-paris-agreement
- https://www.finextra.com/blogposting/18548/why-financial-institutions-must-heed-the-climate-change-risks
- https://www.wsj.com/articles/banks-take-first-steps-on-climate-risk-evaluations-11560538782
- https://www.dw.com/en/climate-change-eu-bank-to-stop-fossil-fuel-lending/a-51258876
- https://www.bloomberg.com/news/articles/2020-02-14/rbs-plans-to-cut-fossil-fuel-loans-be-climate-positive-by-2025
- https://www.sciencedaily.com/releases/2018/09/180924112802.htm
- http://unepinquiry.org/wp-content/uploads/2018/07/Climate_Change_and_the_Cost_of_Capital_in_Developing_Countries.pdf
- https://www.finextra.com/blogposting/18651/managing-climate-change-risks-key-actions-for-financial-institutions
- https://www.reuters.com/article/us-australia-climatechange-banks/australia-plans-new-bank-stress-tests-to-assess-climate-change-impact-sources-idUSKBN2042BC

- https://www.fsb-tcfd.org/about/
- https://www.reuters.com/article/us-climate-change-market-risks/u-s-regulator-homes-in-on-climate-risks-to-u-s-markets-idUSKBN1YF2D5
- https://www.channelnewsasia.com/news/world/united-nations-fight-climate-change-covid-19-12667340
- https://in.reuters.com/article/us-australia-climatechange-banks/australia-plans-new-bank-stress-tests-to-assess-climate-change-impact-sources-idINKBN2042BC
- https://www.reuters.com/article/us-usa-fed-climatechange/fed-has-a-role-in-combating-climate-change-risk-powell-says-idUSKBN1ZT031
- http://www.lse.ac.uk/GranthamInstitute/news/chinas-green-finance-strategy-much-achieved-further-to-go/
- https://www.pinsentmasons.com/out-law/analysis/financial-regulators-focus-on-climate-change-risk
- https://www.bankofengland.co.uk/climate-change

Trend 4: Rising digital adoption in GRC

- https://www.marketsandmarkets.com/Market-Reports/enterprise-governance-risk-compliance-market-1310.html
- https://www.cxotoday.com/press-release/ai-as-a-service-big-data-rpa-to-transform-grc-within-enterprises/
- https://assets.kpmg/content/dam/kpmg/us/pdf/2020/01/integrated-grc-program-bwise-kpmg.pdf
- https://www.chartis-research.com/operational-risk-and-grc/enterprise-grc-solutions-2019-market-update-and-vendor-landscape-11001
- https://www.metricstream.com/grctv/role-of-artificial-intelligence-in-GRC.htm
- https://www.metricstream.com/technology/grc-cloud.ht

Trend 5: Uptake in integrated digital credit risk management solution is rising

- https://www.iif.com/Portals/0/Files/content/Regulatory/11062019_iif_ey_global_risk_survey_2019.pdf
- https://www.prnewswire.com/news-releases/taiwans-first-digital-bank-implements-fully-integrated-kamakura-risk-management-solution-301030161.html
- https://home.kpmg/xx/en/home/insights/2020/03/covid-19-financial-instruments-2b.html
- https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/the-strategic-implications-of-cecl
- https://www.ey.com/Publication/vwLUAssets/ey-ecl-model-of-ar-and-contract-assets-under-ifrs-en/$FILE/ey-ecl-model-of-ar-and-contract-assets-under-ifrs-en.pdf
- http://www.experian.com/business-services/customer-risk-assessment.html
- https://zest.ai/article/zaml-fair-our-new-ai-to-reduce-bias-in-lending
- https://www.ifc.org/wps/wcm/connect/2e1c27bd-2fdd-45be-a82f-7ca00bc3ce78/session_4_florentin_lenoir_lenddo_heure_14h00.pdf?MOD=AJPERES&CVID=INSUUcu
- https://futurism.com/an-ai-completed-360000-hours-of-finance-work-in-just-seconds

Trend 6: Increasing adoption of AI capabilities to fight financial crime

- https://amlabc.com/aml-updates/aml-software/danske-bank-teradata-deploy-ai-to-monitor-fraud/
- https://www.finextra.com/blogposting/14485/to-truly-transform-kyc-and-aml-operations-adopt-ai-and-ml
- https://www.globenewswire.com/news-release/2018/04/16/1471718/0/en/HKEX-Deploys-Nasdaq-SMARTS-Machine-Learning-Technology-for-Market-Surveillance.html
- https://www.niceactimize.com/blog/explainable-ai-the-next-frontier-in-financial-crime-fighting-595/
- https://www.finextra.com/blogposting/16050/ai-and-ml-in-financial-services-compliance-management-use-cases-for-fis
- https://www.reuters.com/article/us-hsbc-ai/hsbc-partners-with-ai-startup-to-combat-money-laundering-idUSKBN18S4M5
- https://www.finextra.com/blogposting/17389/key-ingredients-for-implementing-successful-holistic-trade-surveillance
- https://www.jpx.co.jp/english/corporate/news/news-releases/0060/20180319-01.html
- https://www.finextra.com/pressarticle/73470/hong-kong-stock-exchange-deploys-nasdaqs-smarts
- https://www.therealizationgroup.com/portfolio/the-future-of-trade-surveillance/
- https://www.workfusion.com/customer-spotlight/standard-bank/

Trend 7: Leverage cloud-based managed service offerings to combat financial crime risk

- https://www.niceactimize.com/cloud/cloud-overview/
- https://www.niceactimize.com/blog/financial-crime-managements-broken-system-is-ai-the-answer-585/
- https://www.niceactimize.com/blog/exploring-rpa-in-financial-crime-investigations-from-hype-to-reality-589/
- https://www.niceactimize.com/blog/automating-aml-is-not-a-pipe-dream-were-already-halfway-there-591/

- https://www.infosysblogs.com/cards-and-payments/2018/04/why_i_called_it_fraud_world_of.html
- https://www.infosys.com/newsroom/press-releases/2020/strategic-partnership-financial-crime-solutions.html

Trend 8: LIBOR transition remains a key priority

- https://www.isda.org/2018/02/01/ibor-global-benchmark-transition-roadmap-2018/
- https://www.bis.org/publ/qtrpdf/r_qt1903.pdf
- https://www.pwc.ch/en/publications/2019/How-to-approach-your-LIBOR-transition-web.pdf
- https://www.jdsupra.com/legalnews/the-heat-is-on-regulators-step-up-73811/
- https://www.lexology.com/library/detail.aspx?g=4d7ff561-4c78-4c0a-adfd-17b92d6211f5
- https://www.luxoft.com/blog/cbeer/ibor-transition-a-technology-perspective/
- https://www.moodysanalytics.com/regulatory-news/mar-27-20-fca-communicates-no-impact-of-covid-19-on-libor-transition-date
- https://www.ey.com/en_in/ibor/how-to-address-the-legal-and-contractual-challenges-of-ibor-transition
- https://assets.kpmg/content/dam/kpmg/ie/pdf/2019/07/ie-ibor-reform-transition-new-risk-free-rates.pdf

Trend 9: Continued focus on FRTB implementation

- https://www.dtcc.com/-/media/Files/Downloads/WhitePapers/FRTB-White-Paper.pdf
- https://iflrinsight.com/articles/325/big-banks-take-lead-in-frtb-compliance
- https://www.risk.net/regulation/6830531/the-light-at-the-end-of-the-tunnel
- https://mondovisione.com/media-and-resources/news/eba-publishes-final-draft-standards-on-key-areas-for-the-eu-implementation-of-th/
- https://www.icmagroup.org/Regulatory-Policy-and-Market-Practice/Secondary-Markets/secondary-markets-regulation/fundamental-review-of-the-trading-book-frtb/
- https://www.bloomberg.com/professional/blog/2022-market-risk-odyssey/

Trend 10: Regulatory reporting solution market is growing rapidly

- https://www.marketwatch.com/press-release/regulatory-reporting-solutions-market-top-companies-report-covers-global-industry-break-down-share-growth-trends-and-forecasts-20202025-2020-05-15?tesla=y
- https://www.infosys.com/industries/consumer-package-goods/documents/overcome-regulatory-reporting-challenges.pdf
- https://www2.deloitte.com/content/dam/Deloitte/us/Documents/regulatory/us-banking-regulatory-outlook-2020.pdf
- https://www.apra.gov.au/changes-to-reporting-obligations-response-to-covid-19
- https://www.finextra.com/blogposting/15134/why-regulatory-reporting-continues-to-be-an-achilles-heel-for-fis
- https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2020/regulatory-reporting-covid-19.pdf?la=en&hash=8B7DC0B5B5B0B5563ADCBE54E45FE32A5B561527
- https://www.regulationasia.com/regulatory-reporting-an-approach-for-smaller-banks/
- https://assets.kpmg/content/dam/kpmg/hu/pdf/ten-key-regulatory-challenges.pdf
- http://www.wolterskluwerfs.com/onesumx/commentary/mounting-regulatory-reporting-pressure-in-Asia-Pacific.aspx
- https://www.prnewswire.com/news-releases/finastra-gears-up-for-sftr-with-regulatory-reporting-as-a-service-300912383.html
- https://suade.org/regtech.html

Infosys contributors

Rajneesh Malviya	**Ashok Hegde**	**Amit Khullar**
Senior Vice President, Financial Services	*Vice President, Financial Services*	*Head, Risk and Compliance, Financial Services*

Each contributor mentioned below is a consultant in the risk and compliance area.

Abhisek Bhowmik
Pratik Das
Navdeep Gill
Makarand Dilip Halde
Kartik Jariwala

Anurag Kantak
Anjani Kumar
Mohammed Fayyaz Memon
Nitesh Singh
Naveen Kumar Srivastava

Producers

Samad Masood	**Sharan Bathija**
Infosys Knowledge Institute *London*	*Infosys Knowledge Institute* *Bangalore*

About Infosys Knowledge Institute

The Infosys Knowledge Institute helps industry leaders develop a deeper understanding of business and technology trends through compelling thought leadership. Our researchers and subject matter experts provide a fact base that aids decision making on critical business and technology issues.

To view our research, visit Infosys Knowledge Institute at infosys.com/IKI

Infosys®
Navigate your next

For more information, contact askus@infosys.com

Infosys.com | NYSE : INFY

Stay Connected