MANAGING FINANCIAL RISKS AND COMPLIANCE WITH TECHNOLOGY

Risks have increased for financial institutions during the pandemic, highlighting drawbacks in risk management practices and existing models. For those institutions that can't carve out the extra investment, regulation-as-a-service (RaaS) could be an option.

Infosys® | Knowledge Institute

Heightened risks and aftermath

COVID-19 has increased risks and made them harder to predict. The global economy shrank 3.1% in 2020 vs. 0.1% after the 2008 global financial crisis.[1] According to McKinsey, banks globally could witness a cumulative revenue loss between $1.5 trillion and $4.7 trillion in the time span 2020-2024.[2] Markets too have been significantly volatile. The S&P 500, for example, fell 34% in March 2020, before rising 25% in April 2020. This volatility has hastened regulatory changes in several jurisdictions, widening the regulatory divergence globally. Economic risks and related uncertainties are unlikely to diminish soon.

Managing these risks can be expensive.[3] In 2020, banks worldwide paid US$15 billion in fines for noncompliance. In addition, compliance costs associated with maintaining technology infrastructure and staffing continue to rise.[4] The U.K. banking industry spends between £2 billion to £4.5 billion per year for regulatory reporting alone.[5] This function takes a toll on employee efforts as well. On average, 50%-65% of employee hours are spent on Know Your Customer (KYC)-related data collection and aggregation efforts.[6] These manual efforts stem from siloed data stores and result in inaccurate regulatory submissions.

The sudden economic shakedown has tested financial institutions' risk practices and models. Many risk models have not kept pace with changes in technology, and are therefore ineffective. Institutions must look closely at risk practices and how technologies including artificial intelligence (AI) and cloud can help them.

Typically, banks manage risk practices in-house, which requires significant financial and technological expertise. However, it can be a challenge to keep up with increasing regulatory pressure. Outsourcing a bank's regulatory management is now a potential avenue through RaaS and can be an alternative for those who want to quickly benefit without large investments in talent and tools.

Managing risks efficiently in-house

Banks deal with multiple risks, including market, credit, and cyber-risks. Managing these risks internally poses similar challenges to banks, but each risk has a set of common approaches.

Market risks

During the pandemic, a sudden drop in asset prices increased volatility and market risks. Value-at-risk (VAR) — a popular risk measure — rose to record levels.[7,8] The framework provides a likely single-day loss amount for any asset class or combination of asset classes in a normal market by looking back at the past one year. The fall in financial asset prices led to large trading losses for financial institutions, depleting their collateral values and increasing counterparty risks. Higher market risks require institutions to maintain higher capital levels, constraining their ability to earn from that capital. Banks' risk-weighted assets (RWAs) rose significantly. This is the minimum regulatory capital banks must hold to maintain solvency — the riskier the asset, the higher the risk weight and therefore the higher the capital required. The increase in RWAs also impacted banks' earnings. The net income of the U.S. deposit-taking banks declined 36.5% in 2020, per the FDIC.[9]

The pandemic has increased regulatory scrutiny of risk management practices in banking globally. The Bank of England began examining the impacts of the pandemic on market functioning in early March 2020.[10] The U.S. Federal Reserve Board ruled that banks should treat their trading book losses due to COVID-19 within the market risk capital rule and not as operational losses.[11]

The IT systems that run market risk models have come under stress too. Several underlying market risk modeling assumptions related to valuations and pricing, VAR, RWA, asset and liability management, and liquidity and capital forecasting proved to be less effective in the volatile markets of 2020.

Dealing with market risks

Financial institutions can shift to stressed VAR (SVAR) — a more stable risk measure due to its much longer look-back horizon — to deal with extreme market volatilities. Introduced during the 2008 sub-prime crisis, SVAR was not widely adopted due to insufficient regulatory pressure. However, the pandemic has forced regulators to reevaluate their emphasis on SVAR adoption.

The pandemic has shown that many assumptions on internal market risk-related models are flawed. These must be revised to obtain a more accurate asset valuation and make them fit for stressed times. Capital allocations and hedging strategies must be reviewed, and additional limits should be allocated on trading book sensitivities.

Many institutions still use legacy technologies. This makes it difficult for disciplines that are technology-resource intensive, such as computational finance, and that require high processing power and speed. A shift to digital technologies such as cloud, big data tools, and data lakes can help. When visualized through dashboards, big data analytics can aid in balance sheet risk

management and minimize the impact of macroeconomic fluctuations. For example, RiskSpan, a cloud-based portfolio risk management and analytics solution provider, offers predictive modeling and helps clients in risk analytics management.[12]

Credit risks

Credit risks rose with the pandemic-induced disruptions. Provisioning on loan losses for U.S. and European banks increased by 137% and 113%, respectively, in 2020.[13] Globally, provisions on loan losses rose to US$1.2 trillion by Q3 2020 — up from around US$800 billion in 2019.[14]

2020 saw a substantial decline in lenders' credit quality and underlying collaterals' values. Financially distressed borrowers had to stop or delay their loan payments. Emergency credit applications jumped and recovery rates on loans drastically decreased. Banks' counterparty credit risk also increased due to volatility and reduced asset prices. Credit risk models built on historical data couldn't cope with the pandemic-induced business scenarios.

Managing credit risks

Financial institutions can better manage credit risks by strengthening their credit risk identification, measurement, and monitoring capabilities. Banks need to periodically review their loan portfolios and loan loss provisions under stressed scenarios, avoid credit concentration risks, and recalibrate internal credit risk models.

Digitization through cloud and AI can better integrate credit risk management practices and enhance risk coverage. Application programming interfaces help ingest data from structured (such as transaction and payment history) and unstructured (such as social media activity, mobile phone usage, etc.)

Figure 1: Covid forces a substantial rise in U.S. banking loan loss provisions
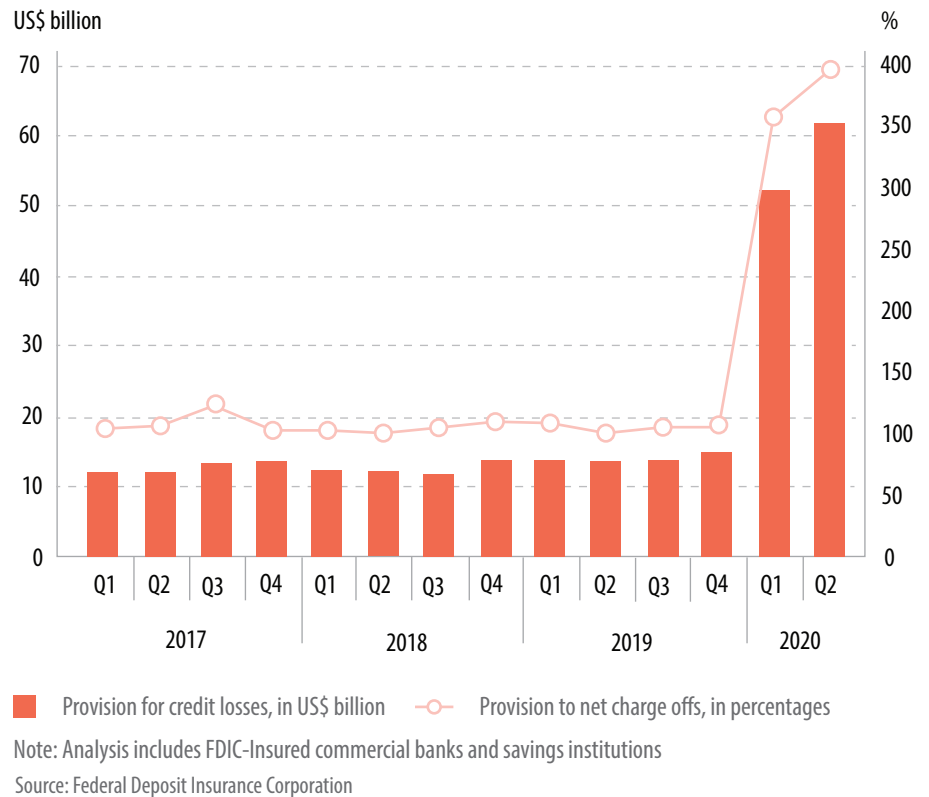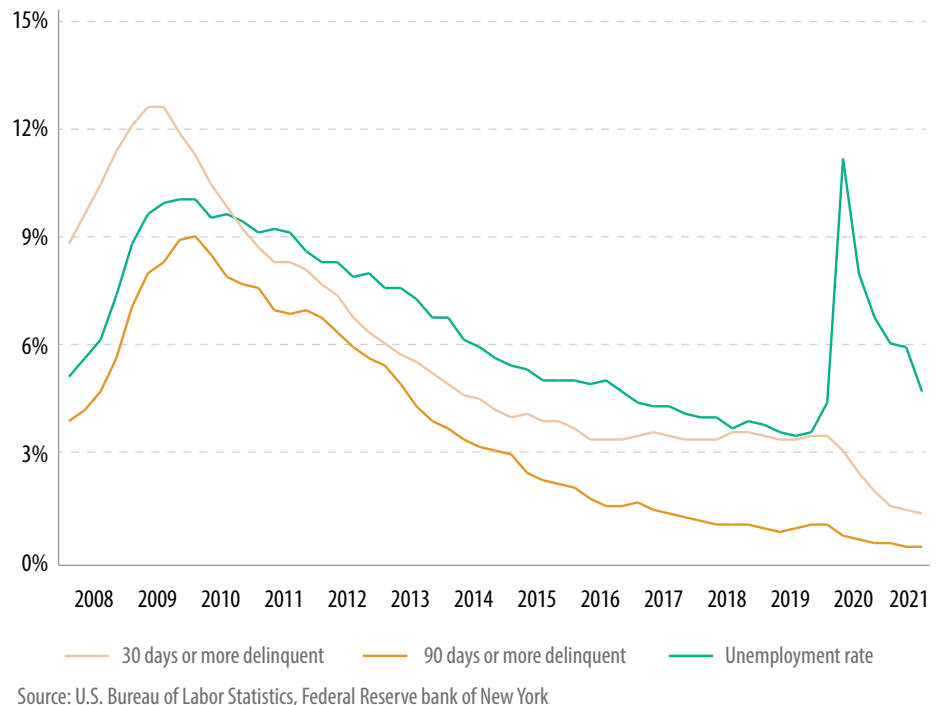

Provision for credit losses, in US$ billion   Provision to net charge offs, in percentages

Note: Analysis includes FDIC-Insured commercial banks and savings institutions

Source: Federal Deposit Insurance Corporation

Figure 2: Unemployment spikes while forbearance cushions mortgage delinquencies post-COVID

30 days or more delinquent   90 days or more delinquent   Unemployment rate

Source: U.S. Bureau of Labor Statistics, Federal Reserve bank of New York

sources.[15] Data analytics enables a 360-degree customer view that helps with better decisioning. For example, OakNorth's credit and monitoring platform is being used by Customers Bank to boost its credit monitoring and portfolio management capabilities. OakNorth's solution combines rich data sets (including unconventional data), cloud computing, and machine learning (ML) capabilities, to provide Customers Bank with deep insights. Customers Bank now gets early warning indicators for credit quality deterioration through 360-degree monitoring of its borrowers' operational and financial data.[16]

Banks strengthen loyalty and establish long-term relationships with their customers by providing proactive measures to their borrowers in difficult times. Citi, for example, waived fines for the early certificate of deposit withdrawal and on monthly service fees for individuals and small-business customers.[17] Another example is Barclays: The bank offered 12-month capital repayment holidays on loans over £25,000. It also launched a

Coronavirus Large Business Interruption Loan scheme to support large corporate banking clients.[18,19]

Technology can also help build goodwill, create customer stickiness, and reduce credit risks. When branches were closed and contact centers were flooded with calls, Nationwide Building Society's customers wanted to apply for mortgage payment holidays. Within days, the institution supported its infrastructure with a trained AI-driven virtual assistant, "Arti," to respond to common COVID-19 mortgage holiday-related queries.[20]

Cyber-risks

Banking cybercrimes have intensified over the years. Cyberattacks rose 238% between February and April 2020 with the growth in digital banking and as cybercriminals took advantage of COVID-19 stimulus payments.[21] Worrying for banks and regulators is that cyber criminals have evolved into organized gangs over time. These criminals leverage malware-as-a-service, execute fileless malware

attacks, and trade in cyberattack tools and services on the dark web. In September 2020, a distributed denial-of-service attack hampered Hungarian banking services when hackers flooded a telecom network with high data traffic.[22]

Cyberattacks can significantly hamper banks, with the average cost of a data breach reaching US$5.7 million in 2021.[23] Even regulators are not immune to these attacks. In January 2021, sensitive information was stolen from New Zealand's central bank due to a breach from a third-party file-sharing service.[24] These attacks can impact a country's overall banking system. The Federal Reserve Bank of New York estimates that an attack on any of the five most active banks in the U.S. could affect 38% of the country's banking network.[25]

Financial institutions' traditional and siloed legacy cybersecurity systems don't help in such scenarios, as they lack robust identity, access management capabilities, and real-time monitoring.

Managing cyber-risks

Regulators are taking several measures to better manage cybercrimes and bring in more transparency. U.S. regulators now require banks to report cybersecurity incidents within 36 hours of a breach being identified.[26] Cyber insurance laws are also being strengthened. In February 2021, the New York State Department of Financial Services issued a new cyber insurance risk framework outlining the industry's best practices — the first guidance on cyber insurance by a U.S. regulator.[27] In the European Union, PSD2 strong customer authentication requirements came into force in 2021 to curb frauds in online and contactless offline payments.[28]

Financial institutions must keep pace with the emerging trends and regularly assess their cyberhealth. Various cybersecurity policies, procedures,

Figure 3. The number of compromises continues unabated

In numbers
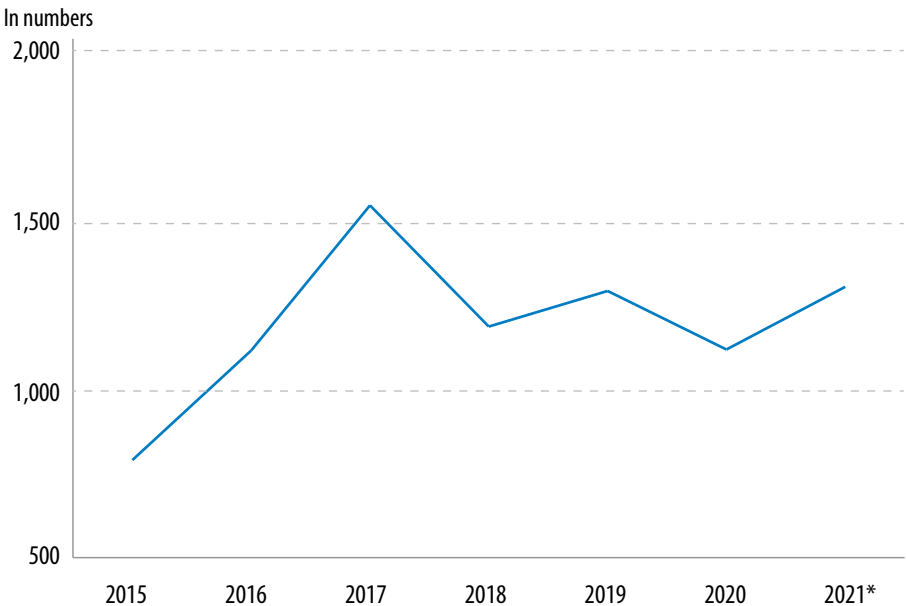
* As of September 2021

Note: Compromises includes data breaches, data exposures, data leaks and unknown attack vectors

Source: Identity Theft Resource Center

and solutions must be implemented. All stakeholders must be continuously educated and trained on cybersecurity best practices.

AI capabilities such as ML, robotic process automation and natural language processing can reinforce cybersecurity defenses.[29] These technologies can be applied to prevent zero-day attacks, risk quantification, intrusion detection, threat hunting and penetration testing, and alert investigation. For example, FICO's ML-based Cyber Risk Score solution utilizes globally gathered micro signal data to quantify an organization's potential cyber-risk over a 12-month period. The score helps measure breach exposure and security posture.[30]

An alternative to managing regulations in-house

Not all banks want to manage risks in-house; some prefer to outsource. That's when the RaaS model could be a solution — and better suited for banks with smaller regulatory reporting teams. RaaS shifts the compliance affairs to experts and reduces the initial investment required for compliance management. This way, banks can manage compliance proactively and efficiently and shift their focus to customers.

RaaS is efficient and cost-effective

RaaS can significantly improve the overall performance of a financial institution's regulatory compliance functions. As per estimates, the model can reduce the operational effort by up to 80%. RaaS engagements can be formed for a specific or an end-to-end regulatory operation or function. Its multi-tenanted architecture offers improved cost optimization and predictability. The model shifts spending from capex to opex, reducing costs by 35%-60%, according to estimates. A KYC operation alone is estimated to cost large global financial institutions US$150 million per year on average.[31]

Under the RaaS model, the regulatory compliance operation is outsourced under a subscription- or outcome-based model to a cloud-based managed service provider. The provider takes on the management, execution, and transformation of compliance operations. This includes enabling the required technology, hosting platforms, and compliance applications. For example, six Nordic banks allied to offer KYC-as-a-service.[32] The platform standardizes processes for handling KYC data and helps in AML and financial crime prevention. It also delivers efficient and accurate processes to serve customers, banks, and society.

RaaS providers offer advanced digitalization capabilities, cloud-based workflow engines, high computational power, accelerators, and dashboards. They leverage databases (such as Equifax, Dun & Bradstreet), and other publicly available sources, for compliance activities. For instance, Finastra's private cloud-hosted solution gathers and inspects transaction data from banks' own or third-party systems.[33] It allows banks to efficiently handle new and changing regulatory reporting requirements, such as those related to SFTR, MiFID II, and EMIR.

Pick the perfect model that best deals with risks

Financial institutions need to strategically analyze and adopt the model that best suits their specific needs. For institutions that find it difficult to carve out investments, RaaS is the best fit. Yet, a few banks are hesitant to adopt RaaS, as they prefer to control risk and compliance functions internally, while others have to deal with deeply entrenched legacy systems and are less confident in cloud security.

Whichever model banks choose, technologies such as cloud and AI must be at the core. This bolsters their capital position, strengthening their operational and cyber resilience and fortifying their risk management and regulatory compliance capabilities.

Figure 4. The number of malware attacks continues to remain high

In millions
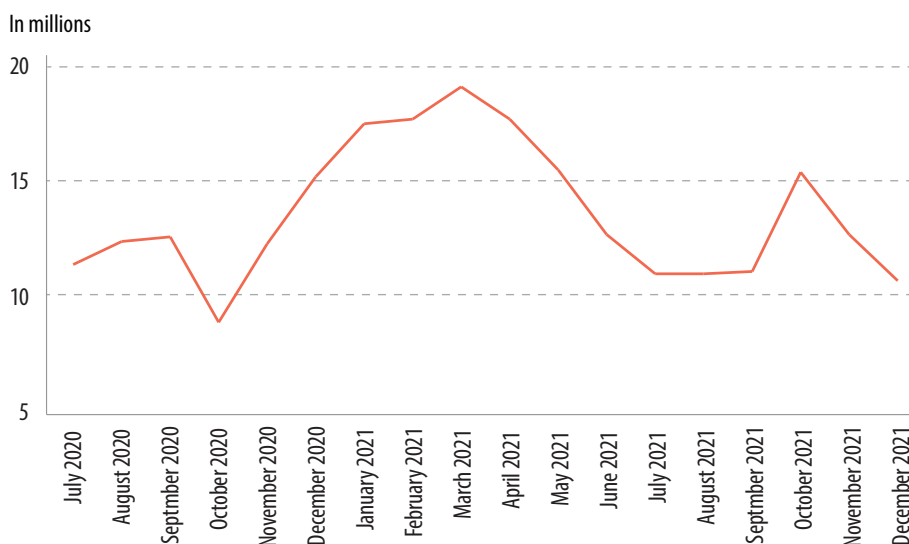
Source: AV Test

References

1. Global recovery continues, but the momentum has weakened and uncertainty has increased, October 2021, IMF.

2. The great divergence - McKinsey's Global Banking Annual Review, Dec. 1, 2021, McKinsey.

3. AI: The New Way of Doing KYC and AML, Anjani Kumar, Harry Keir Hughes, March 2021, Infosys Ltd.

4. Banks Worldwide Amass $15B in Fines in 2020, U.S. Banks Account for 73%, Jan. 11, 2021, Corporate Compliance Insights.

5. Future of Finance: Review on the outlook for the UK financial system, Huw van Steenis, June 2019, Bank of England.

6. Reducing the cost of compliance: A bold move towards Know Your Customer (KYC) managed services, October 2018, Thomson Reuters.

7. The long-term effect of Covid-19 on market risk capital, Louie Woodall, Sept. 8, 2020, Risk.Net.

8. Goldman Sachs' VAR hits five-year high, Louie Woodall, April 15, 2020, Risk.Net.

9. FDIC-Insured Institutions Reported Net Income of $59.9 Billion In Fourth Quarter 2020, Feb. 23, 2021, FDIC.

10. Governor statement to Treasury Select Committee, on behalf of the FPC, MPC and PRC, March 3, 2020, Bank of England

11. COVID-19 Supervisory and Regulatory FAQs, Board of Governors of the Federal Reserve System.

12. RiskSpan Wins Risk as a Service Category for Second Consecutive Year, Leaps 12 Spots in RiskTech100® 2022 Ranking, Nov. 15, 2021, RiskSpan.

13. Global Risk 2021: Building a Stronger, Healthier Bank, Gerold Grasshoff, Matteo Coppola, Bernhard Gehra, et al. May 12, 2021, BCG.

14. Global banks steel themselves against larger potential loan losses than seen in the Great Recession, Dec. 17, 2020, McKinsey.

15. Leveraging Artificial Intelligence & Machine Learning in Credit risk management, Anjani Kumar, Pratik Das, 2020, Infosys Ltd.

16. Customers Bank enlists OakNorth to boost credit monitoring and portfolio management, April 8, 2020, Finextra.

17. Citi Assists U.S. Customers and Small Businesses Impacted by COVID-19, March 6, 2020, Citi Group.

18. Barclays offers repayment holidays to corporate borrowers hit by coronavirus, March 10, 2020, Reuters.

19. Supporting our customers and clients impacted by coronavirus (COVID-19), July 2, 2021, Barclays.

20. Coronavirus: Nationwide's human expertise used to quickly build smart agent amid pandemic, Karl Flinders, May 12, 2020, ComputerWeekly.com.

21. Attacks on Banks Spike 238% During #COVID19 Crisis, Phil Muncaster, May 15, 2020, Info Security Group.

22. Hungarian banks, telecoms services briefly hit by cyber attack: Magyar Telekom, Sept. 26, 2020, Reuters.

23. Cost of a Data Breach Report 2021, 2021, IBM.

24. New Zealand central bank hit by cyberattack, Jan. 10, 2021, Deutsche Welle.

25. Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis, Thomas M. Eisenbach, Anna Kovner and Michael Junho Lee, May 2021, Federal Reserve Bank of New York

26. Federal Regulators Adopt New Computer-Security Incident Notification Requirements for Banks and Service Providers, Dec. 2, 2021, JD Supra

27. Superintendent Lacewell Announces DFS Issues Cybersecurity Insurance Risk Framework, Feb. 4, 2021, Department of Financial Services.

28. Why it's time for merchants to take control of the road to PSD2 SCA, Sept. 24, 2020, The Paypers.

29. AI and ML in Cybersecurity Risk Management, Anjani Kumar, Amit Khullar, December 2020, Infosys Ltd.

30. FICO Releases Machine-Learning Cyber Risk Score on AWS Marketplace, Nov. 6, 2019, PR Newswire.

31. Reducing the cost of compliance: A bold move towards Know Your Customer (KYC) managed services, October 2018, Thomson Reuters.

32. Six Nordic banks form alliance to offer KYC as a service, Gerard O'Dwyer, July 30, 2019, ComputerWeekly.com.

33. Finastra Gears up for SFTR With Regulatory Reporting as a Service, Sept. 5, 2019, PR Newswire.

Author

Anjani Kumar

Principal Consultant

Financial Services, Domain Consulting Group

Contributors

Abhishek Prasad Mokal

Senior Consultant

Financial Services, Domain Consulting Group

Pankaj Jaiswal

Senior Consultant

Financial Services, Domain Consulting Group

Kartik Jariwala

Senior Consultant

Financial Services, Domain Consulting Group

Poonam

Lead Consultant

Financial Services, Domain Consulting Group

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 or email us at iki@infosys.com.

For more information, contact askus@infosys.com

Infosys.com | NYSE : INFY

Stay Connected