Deloitte.

India Banking Fraud Survey Edition IV

January 2022

Contents

Preface

We, Deloitte Touche Tohmatsu India LLP (Deloitte India) are proud to present the fourth edition of our India Banking Fraud Survey. Our endeavour with every edition of the survey is to bring key issues being faced by the banking sector to the fore. When we launched our third edition in 2018, none of us had envisioned that the next release of this report would be at what we hope is the end of a global pandemic.

The impact of COVID-19 has resulted in organisations and regulators across the globe operating in an entirely new environment. Whilst we adjust to the new normal, there will be those who will look to exploit gaps and weaknesses in the systems. Financial crime across the globe is expected to rise in response to the uncertainty in the business landscape. For banks, the economic slowdown has only heightened the risk of fraud and money laundering. Banking sector regulators have been at the forefront of fraud mitigation strategies, prescribing frameworks that banks need to adopt to identify and mitigate fraud risks.

As new risks begin to emerge, banks need to remain vigilant to ensure they continue to effectively mitigate them. Banks that can utilise technology to enhance their operations can stay on top of preventive, detective, and enforcement measures, thereby effectively guarding themselves against increasingly complex financial crimes.

With this backdrop, the fourth edition of the Deloitte India Banking Fraud Survey attempts to understand banks' mechanisms to tackle fraud risks, the impact of new operational models on fraud risk management, and perspectives on making strategic investments for the future.

We hope that the survey report will influence discussions and debate amongst banks, regulators, and practitioners on how to tackle (and improve) fraud and compliance risks being faced today. In any scenario, the industry must prepare for the next normal to be very different from that of the past ten years, for which, this report is intended to provide strategic direction.

KV Karthik
Partner and Lead -
Financial Crime Compliance,
Forensic, Financial Advisory
Deloitte India

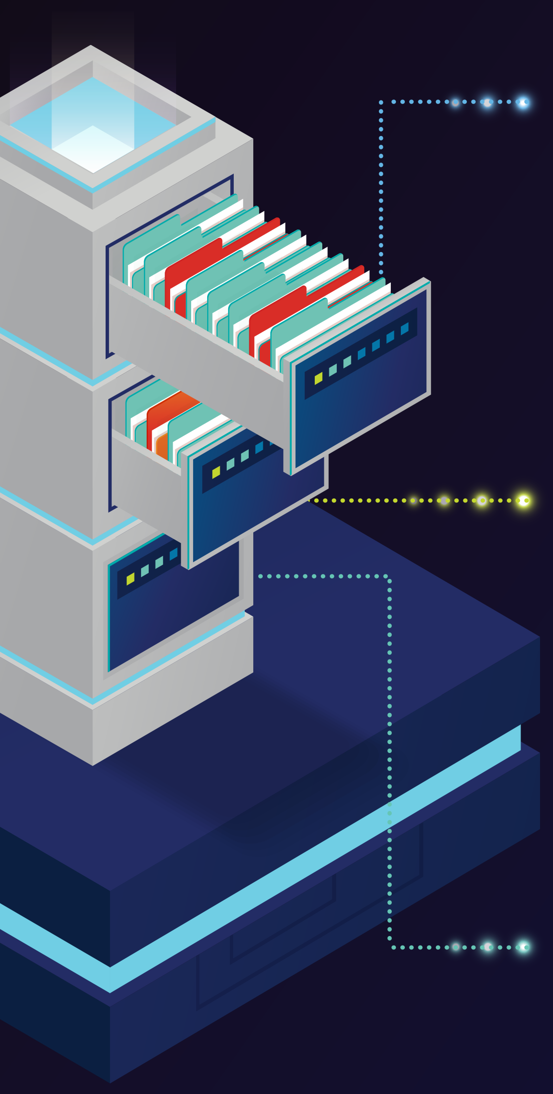
Nishkam Ojha
Partner
Forensic,
Financial Advisory
Deloitte India

Executive summary and key findings

A comparison of some of the key findings from our previous editions indicate that while technology (if in the wrong hands) could be used to circumvent bank systems, it can also be an effective tool to keep ahead of and identify/detect fraud risks.

78%

respondents believe that frauds in the banking sector will increase over the next two years



	Top three responses on the factors responsible for the increase in fraud incidents over the next two years	Top three responses on how a fraud incident is typically detected	Top five responses on the types of fraud experienced over the last two years
2021	• Large-scale remote working models • Increase in customers using non-branch banking channels • Limited/ineffective use of forensic analytics tools to identify potential red flags	• During routine account audit/reconciliation or process reviews • Through internal automated data analysis or transaction monitoring software • Through a customer complaint/an internal whistle blower complaint	• Data theft • Cybercrime • Third-party induced fraud • Bribery and corruption • Fake/fraudulent documentation
2018	• New technology/digital channels that make fraud detection difficult • Lack of forensic analytics tools to identify potential red flags across different processes • Business pressure to meet targets	• During routine account audit/internal audit/reconciliation • Through a customer complaint • Through an internal whistle blower complaint/through internal automated data analysis or transaction monitoring software	• Fraudulent documentation • Cybercrime • Overvaluation/non-existence of collateral • ATM skimming/fraud • Siphoning/diversion of funds
2015	• Lack of oversight by the line manager or senior management on deviations from existing processes • Business pressure to meet targets • Lack of forensic analytics tools to identify potential red flags across processes	• Through a customer complaint • During routine account audit/reconciliation • Through an internal whistle-blower complaint	• Diversion/siphoning of funds • Fraudulent documentation • Incorrect financial statements • Over valuation/absence of collateral • Identity theft

Some other key survey findings to note are:

What kind of fraud risks are currently the biggest concerns for your bank?

(The top four responses have been highlighted)

24% Loan frauds

14% Mobile / Internet banking frauds

13% Identity / data theft

9% Phishing

What will be some important outcomes of COVID-19 on your banks' Fraud Risk Management (FRM) function?

(The top three responses have been highlighted)

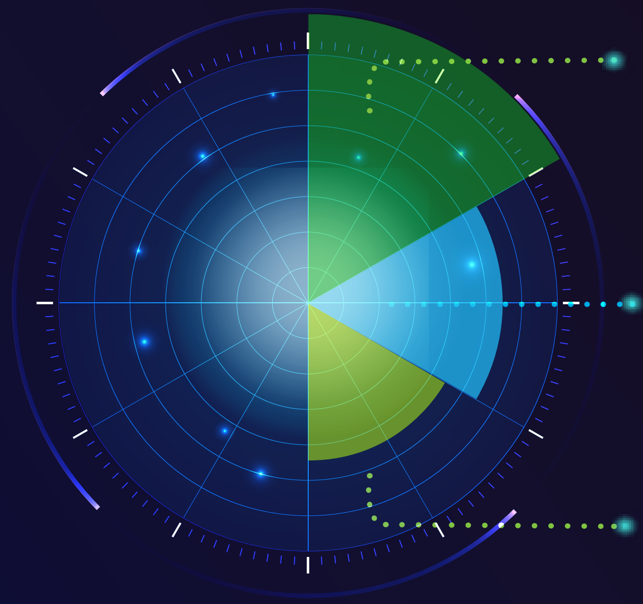
25% Increased dependence on analytical tools for fraud monitoring and detection

23% Creating increased awareness on fraud among customers and employees

21% Change in target operating model to enhance capabilities of the remote FRM function

Over the last six months, what measures has your bank implemented to mitigate fraud?

(The top three responses have been highlighted)



23% Optimized existing EWS and fraud monitoring systems to cater to current banking conditions, using AI/ML and by integrating external databases

18% Enhanced case management solutions to effectively respond to fraud incidents and report on time

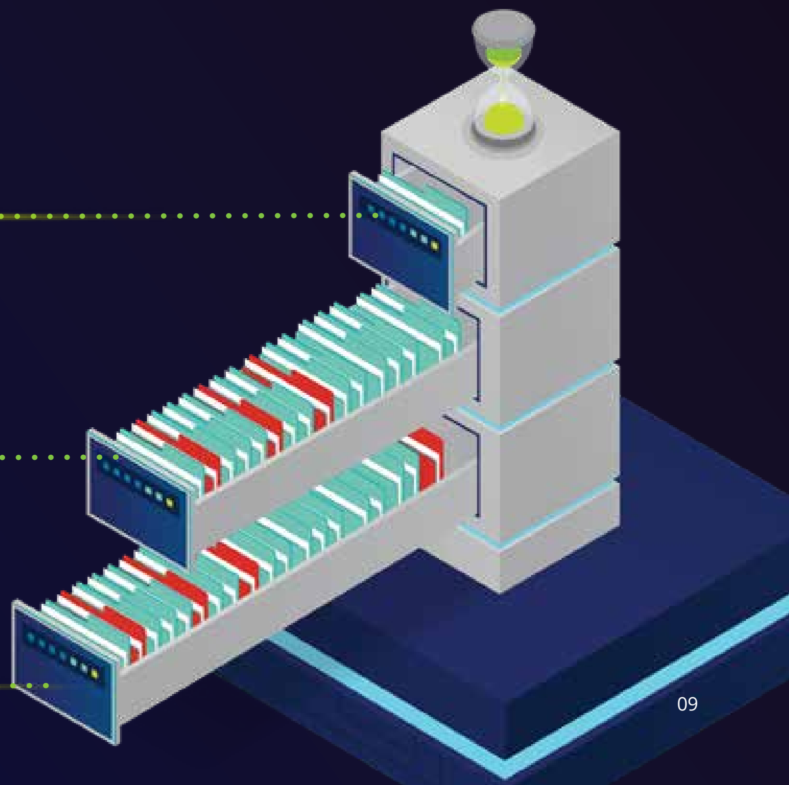
17% Arranged trainings/workshops to upskill staff involved in fraud-monitoring functions

How frequently does your bank conduct fraud risk assessments and update the fraud risk register?

5% Haven't done so in the last five years

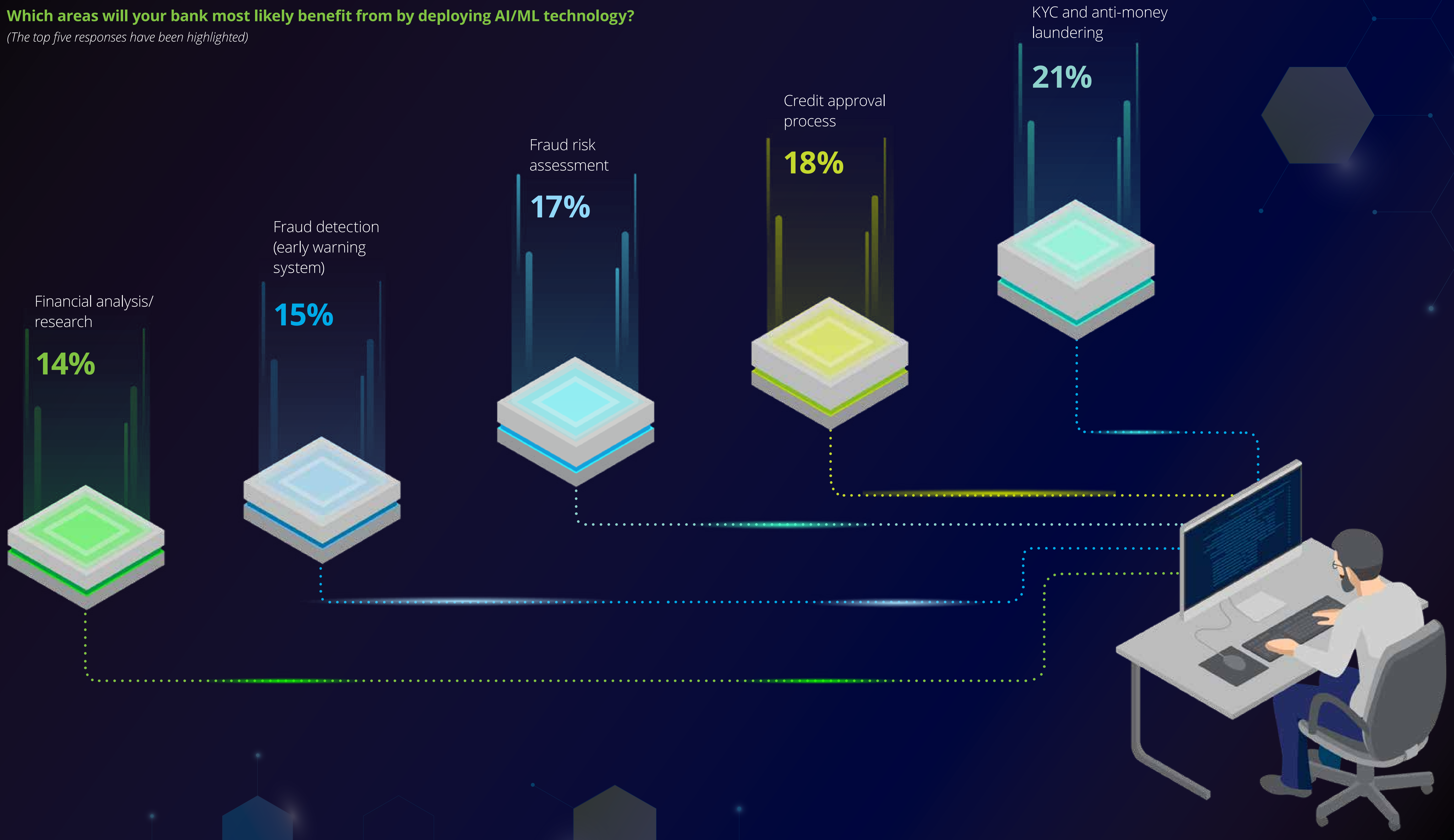
45% Once in two/three years

50% Once a year



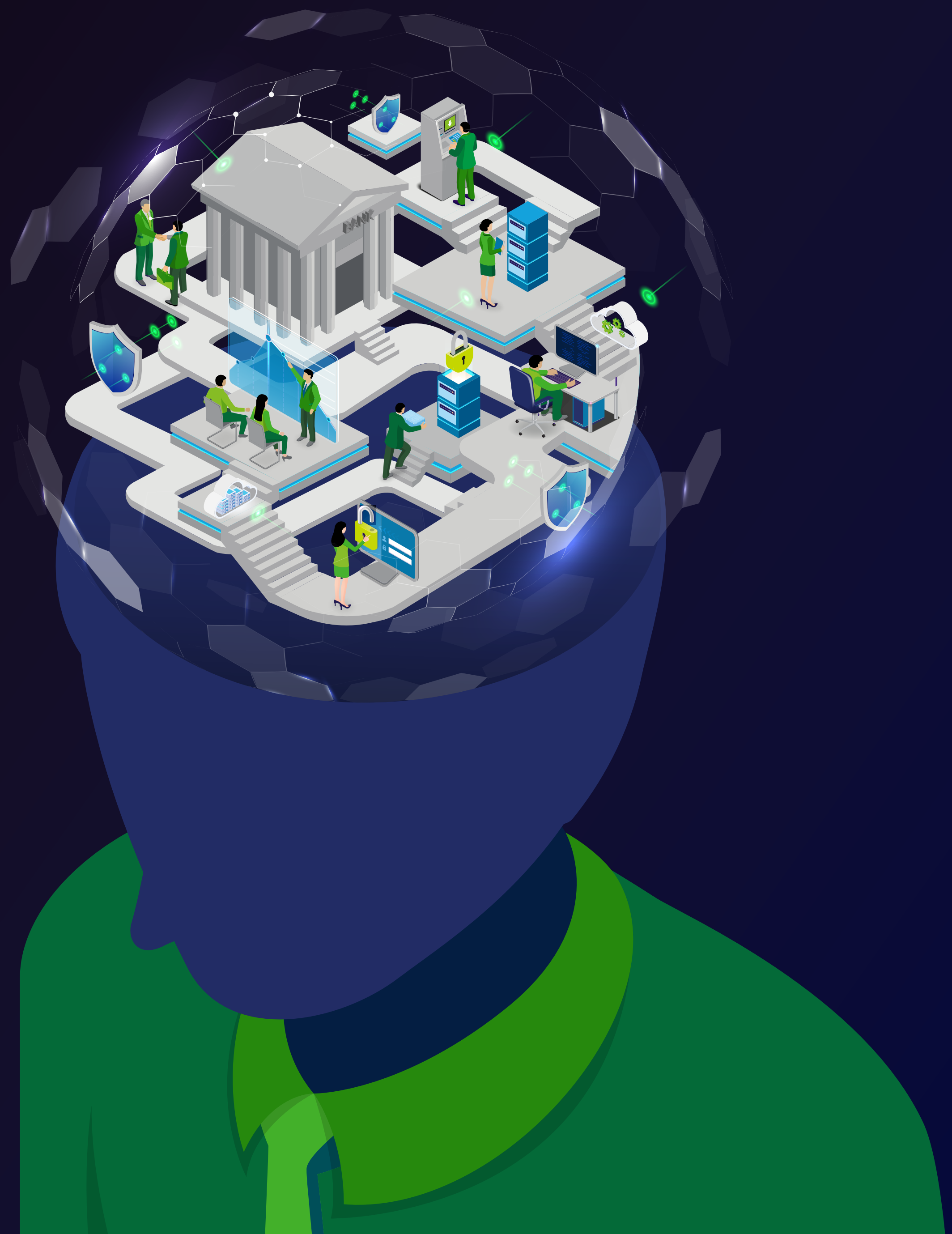
Which areas will your bank most likely benefit from by deploying AI/ML technology?

(The top five responses have been highlighted)



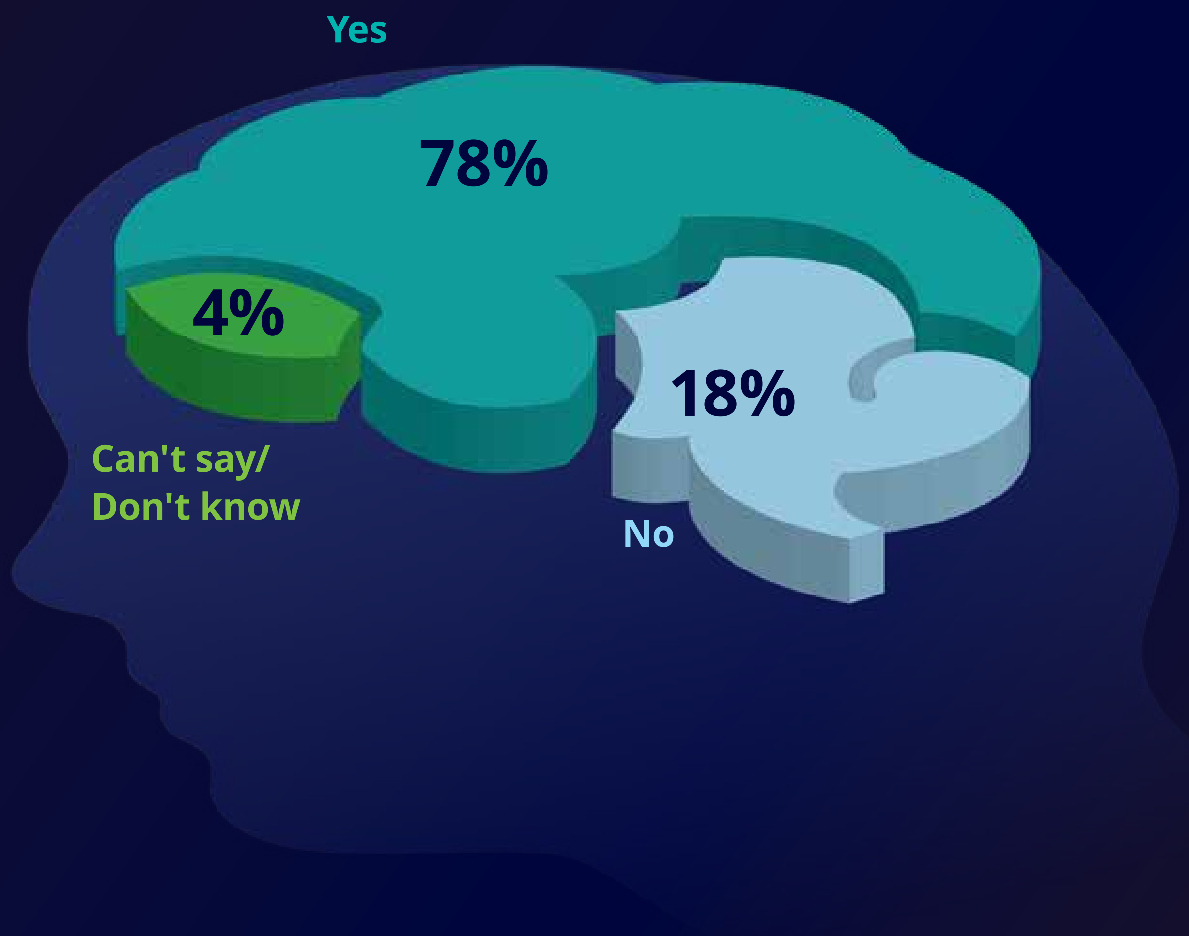
Section I

Understanding the current fraud environment in the banking sector



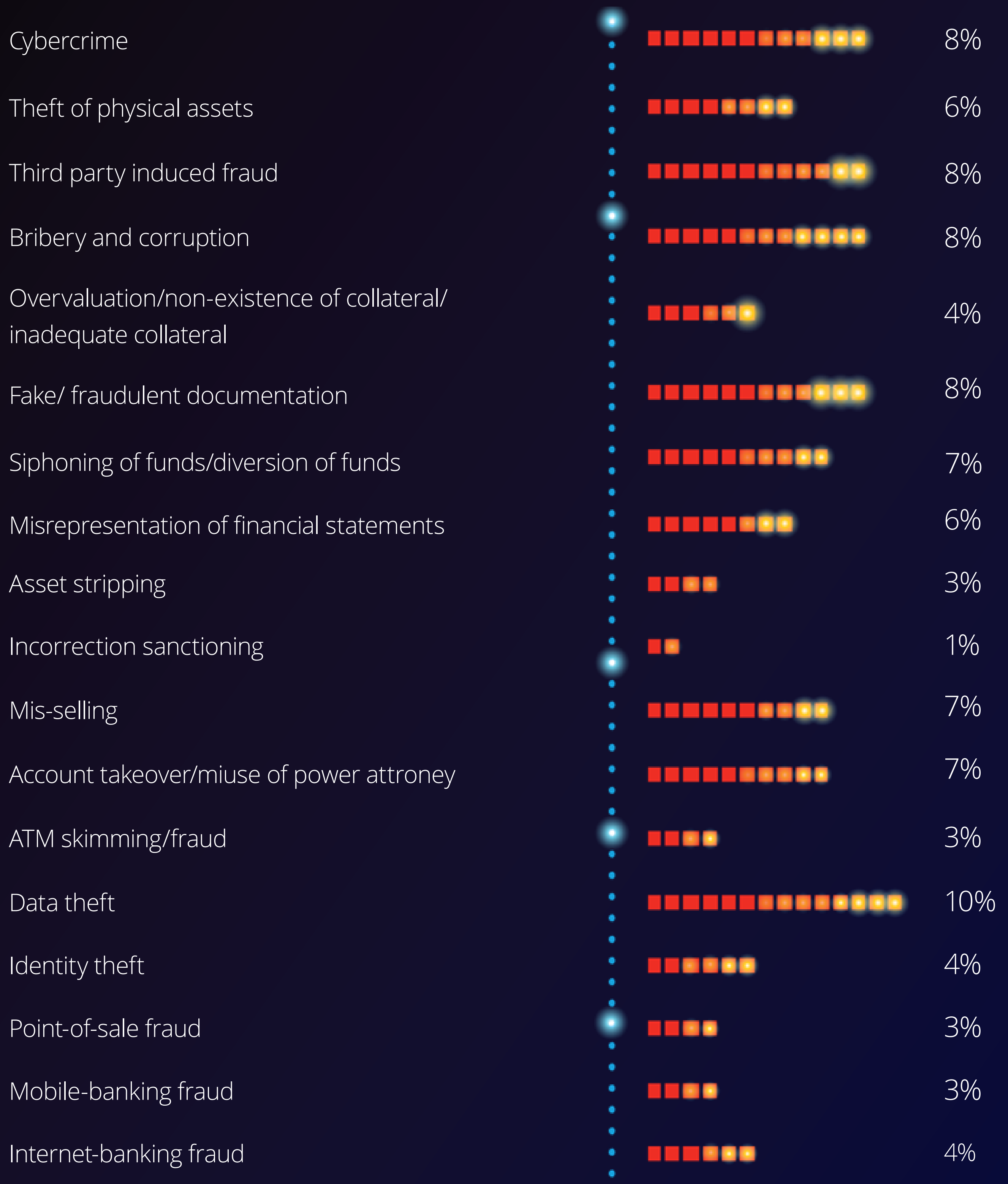
a) Trend analysis

Do you believe that the current business disruption due to the pandemic can spur banking sector frauds over the next two years?



COVID-19 came at a time when banks were struggling to deal with an increasing number of fraud incidents. Banks were facing a three-pronged “attack” in combatting financial crime: **Growth in digital transactions, continually evolving regulatory guidelines, and new fraud trends.** While banks are yet to fully understand the implications and impact of the current environment on fraud-related matters, there appears to be acceptance on part of the banks that the pandemic may possibly lead to a rise in frauds with 78 percent respondents stating that frauds could increase over the next two years.

Which of the following types of frauds has your bank experienced in the last two years?



Over the course of the last few years, there has been a major push towards financial inclusion and digitisation, making both consumers and banks rely heavily on electronic channels for banking. This has only further intensified during the pandemic and may likely continue to increase.

No doubt, the recent changes/ technological advancements brought about by the pandemic will have a lasting impact on the banking industry. In addition, it is highly likely that further changes may be warranted in the future in the way the banking industry operates.

In line with these trends, data theft, cybercrime, third-party induced fraud, bribery and corruption, and fraudulent documentation have been identified as the top five concerns with over 42 percent of respondents (cumulative) reporting to be victims of these.

Comparison with the responses to our previous survey, risks such as data theft and bribery and corruption have now come to the forefront. There is a noticeable increase in these fraud types. With a shift in these trends, banks should make a concerted effort to proactively identify the root cause of these fraud risks to be better prepared in the future. Increasing instances of data theft and cybercrime could be especially alarming for banks, as this could have a negative impact on consumer confidence and trust.

b) Impact of COVID-19

COVID-19 forced both the Reserve Bank of India (RBI) and financial institutions to take measures to counter its disruptive effects. In response to the pandemic and to help rejuvenate the economy, the RBI and the Government of India announced a wide variety of initiatives. Amongst these were the moratorium on loan re-payments, the interim freeze on Insolvency and Bankruptcy Code (IBC) cases, and bank loan restructuring to name a few.

Banks too had to adapt to the restrictions that resulted from the pandemic. Lockdowns and social distancing norms restricted the mobility of bank staff and customers, thereby increasing the reliance on digital channels and other forms of non-face-to-face banking services. With a significant number of bank staff working from home, banks had to provide their staff remote access to their organisation's network and information. This forced banks to enact significant organisational and operational changes within a short timeframe to avoid service interruptions; posing a worrying question—have all such changes been assessed for their vulnerability to fraud?

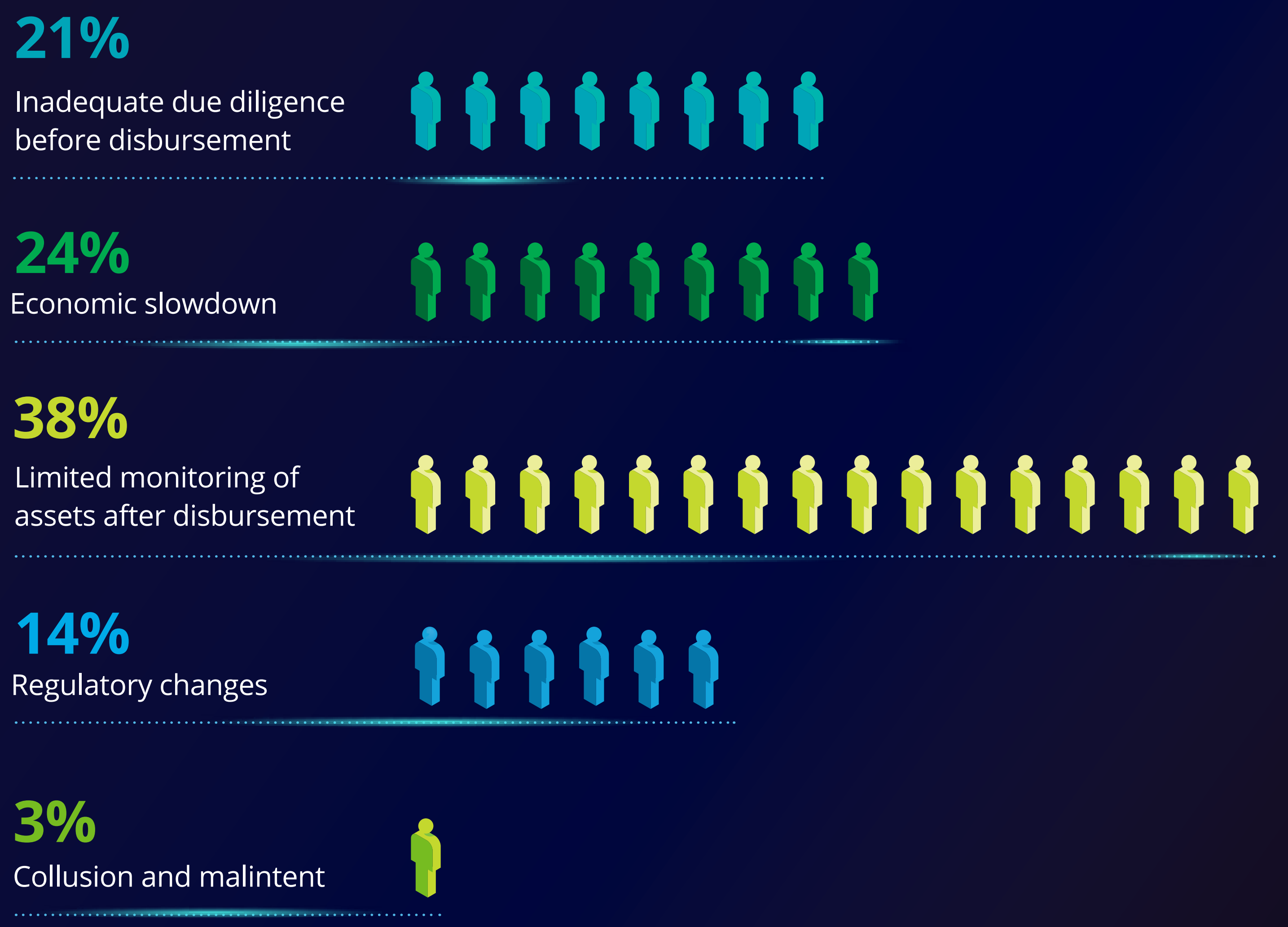
With myriad changes being deployed at the front-end but processes and systems possibly remaining untouched, have banks been exposed to undiagnosed vulnerabilities? Due to the advent of new digital touchpoints between banks and their customers for various contactless banking and other services, banks must take the necessary steps to understand how these changes will impact their fraud readiness.

According to industry experts, new loans and loan extensions are expected as a result of the government's stimulus package for MSMEs as well as the RBI moratorium. Banks will need to be extra vigilant while granting facilities or renewing existing facilities, taking into consideration the stress in the account and viability of the business amidst the changed scenario.

With changes caused by the pandemic continuing to persist in more ways than one, banks will need to be more agile in implementing change swiftly without comprising on risk management.

c) Stressed assets

What do you believe has led to higher stressed assets?



Stressed assets continue to be an area of concern for banks, with the pandemic adversely impacting specific industries. Respondents have cited limited asset monitoring after disbursement (38 percent), the economic slowdown (24 percent), and insufficient due diligence prior to disbursement (21 percent) as the top three factors leading to higher stressed assets. These suggest that banks may need to overhaul their due-diligence and monitoring frameworks.

For the overall effectiveness of asset monitoring frameworks, banks should consider an integrated approach that applies the findings of pre-disbursement due diligence to on-going monitoring and identifies anomalies and red flags. In this approach, it is critical that the level of due diligence conducted has accurate, extensive, and actionable intelligence. In the post-disbursement phase, monitoring needs to be robust and all-encompassing of EWS, new fraud scenarios, and integrating intelligence gathered from internal and external data sources.

Section II

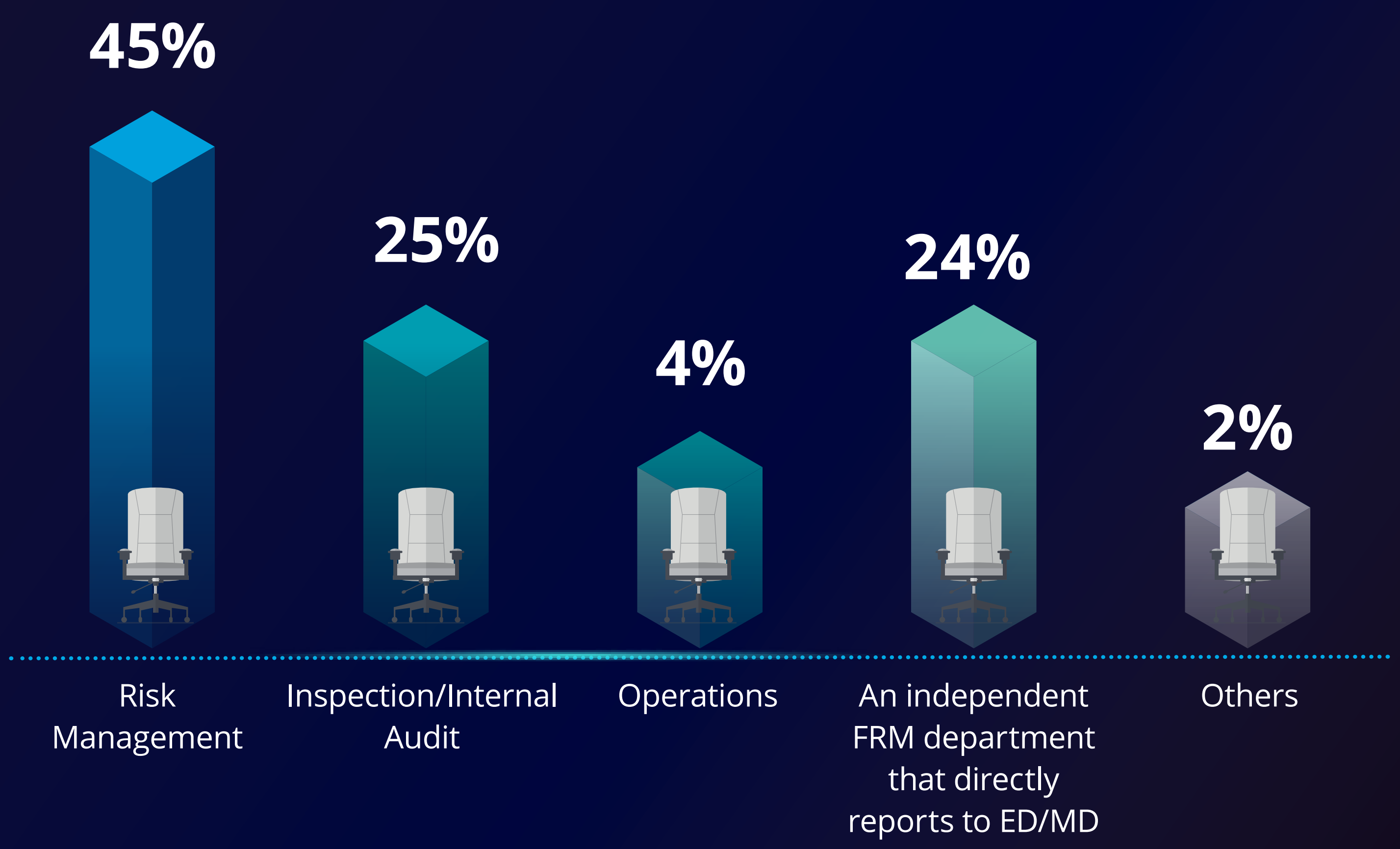
Fraud risk management and continuous monitoring at banks

a) Current FRM governance and structure

Aligning the FRM function within a bank's organisational structure

Only 24 percent respondents mentioned that their FRM department reports directly to the ED and MD. Additionally, about 45 percent and 25 percent respondents stated that the FRM department was a part of the Risk Management and Internal Audit/Inspection functions of the bank, respectively.

In your bank, which department does the fraud risk management (FRM) function report to?



For an FRM function to be effective, in addition to a strong and robust Enterprise Fraud Risk Management (EFRM) solution, a bank should have a dedicated and independent team with a strong compliance culture. The FRM department should look to manage three pillars viz., governance, prevention/detection/investigation, and reporting. This includes having an efficient fraud monitoring system that takes into consideration inputs from inspection, credit monitoring, business, etc. teams; having a skilled pool of fraud risk management officers; reporting fraud and enhancing policies, procedures, and updating risk registers on a timely basis to avoid reoccurrence.

In your bank, which of the following activities is a responsibility of the FRM function?

(Respondents chose all applicable options)

26%	Prevention and detection of frauds
25%	Investigation and preparation of investigation reports
29%	Reporting of fraud cases to internal and external stakeholders
20%	Fraud risk review before approval for launching new products/ services and processes

A strong fraud risk management/fraud monitoring function can help banks minimise the impact of fraud, thereby reducing losses and safeguarding their reputation. It should be able to prevent/ detect/ investigate multiple types of fraud risks, while having the ability to prepare for new regulations as well as tackle emerging fraud risks.

The need for an independent FRM Unit

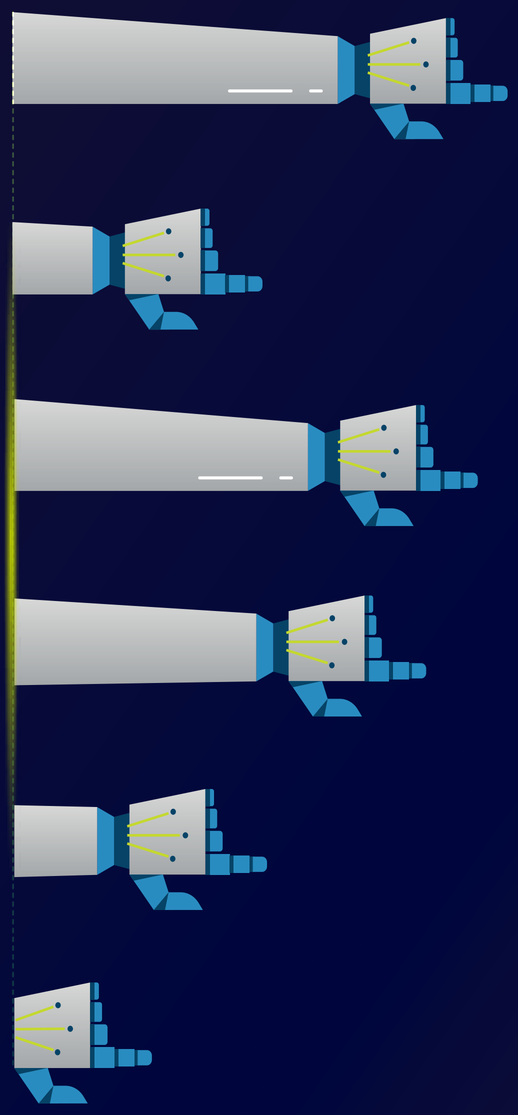
Having an independent FRM department reporting directly to the ED/MD/CEO of the bank has many advantages, the most important being communicating the importance that the senior management places on the FRM function. A second benefit is the conflict of interest avoidance when performing FRM functions. It contributes to the development of new products/ services, process optimisation, skill development, etc., by bringing in aptly skilled resources in an independent FRM unit. An independent FRM unit can also help avoid delays in decision making, especially in large value frauds, and promptly bringing it to the senior management's notice.

However, apart from aligning the FRM unit, it is critical to create and reinforce a culture with zero tolerance for fraud within the organisation's DNA. Active involvement and oversight by the senior management/board can help set the right tone at the top. Creating a zero-tolerance culture also involves communicating this message and demonstrating the focus required from senior management. In addition, in line with the RBI,[1] the fraud risk management, fraud monitoring, and fraud investigation function must be owned by the bank's CEO, audit committee of the board, and the special committee of the board.

[1] Source: https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=10477

b) Current status of the implementation of anti-fraud programmes

What do you feel will be the most important outcome of COVID-19 on your FRM function?



25%	Increased dependency on analytical tools for fraud monitoring and detection
13%	Increase in dedicated manpower for evaluating fraud alerts
23%	Creating increased awareness on fraud among customers and employees
21%	Change in target operating model to enhance capabilities of the remote fraud-risk management function
13%	Increased regulatory scrutiny
5%	Increased cost of investigation and damage control

According to 25 percent respondents, the most important impact of the pandemic on fraud risk management functions has been increased dependency on analytical tools for fraud monitoring and detection. Using data analytics as part of fraud risk management may be indicative of a shift in the banking industry. The pandemic has resulted in staff shortage, increase in contact-less operations and services, and remote operations increasing the need for data analytics-oriented fraud risk management solutions. This is evident by 21 percent respondents highlighting that changes in their target operating model to enhance capabilities of the remote fraud-risk management function will also be an outcome of the pandemic.

How many fraud incidents has your bank encountered in the last two years?

Retail Banking

Less than 100	29%
Between 100 and 200	29%
More than 200	25%
No incidents	10%
Unaware	7%

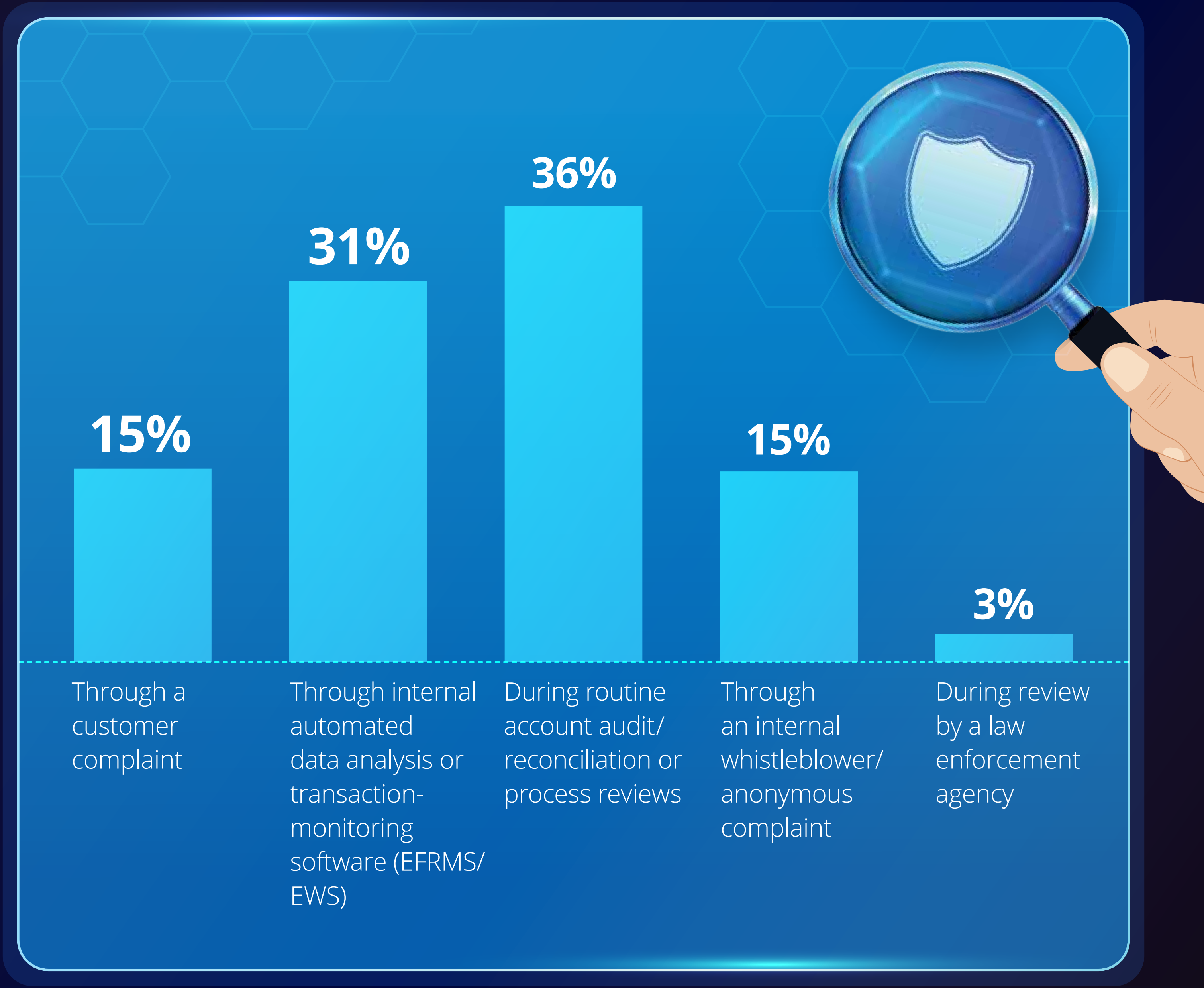
Non-Retail Banking

No incidents	12%
Less than 10	20%
Between 10 and 20	12%
Between 20 and 50	37%
More than 50	19%

The number of fraud incidents encountered by banks over the last two years appears to have increased, compared with the findings of our previous survey. Fifty-three percent respondents indicated that they have faced more than 100 fraud incidents in retail banking (over the last two years)—a 29 percent increase since the previous edition.

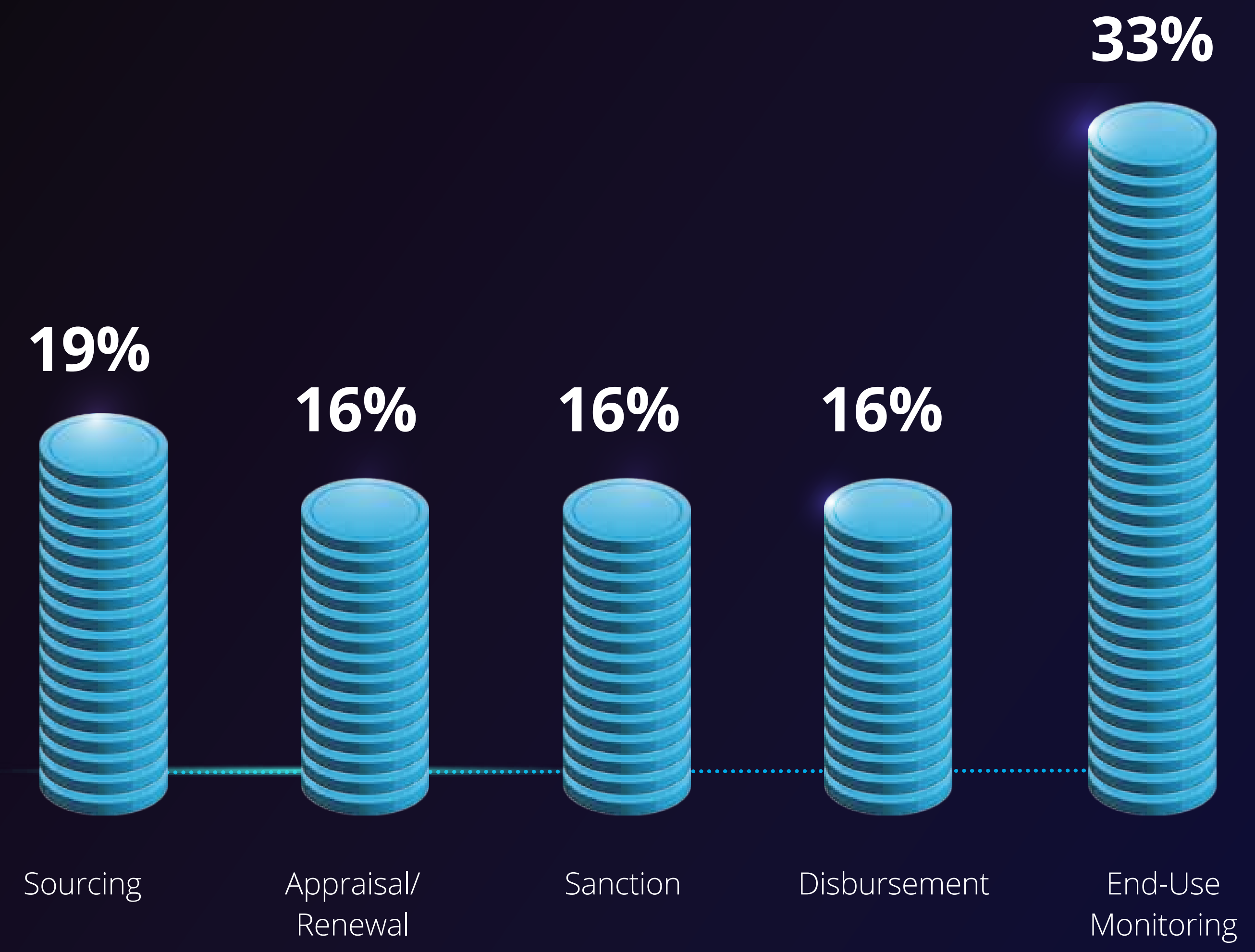
Similarly, in the non-retail business, the current survey highlighted that 56 percent respondents encountered more than 20 fraud incidents; while in the previous edition, a similar number of incidents were experienced by 22 percent respondents. Fraud controls and mitigation strategies should therefore be a significant priority due to the sheer rise in fraud incidents and the consequential losses incurred.

How is a fraud incident currently detected in your bank?



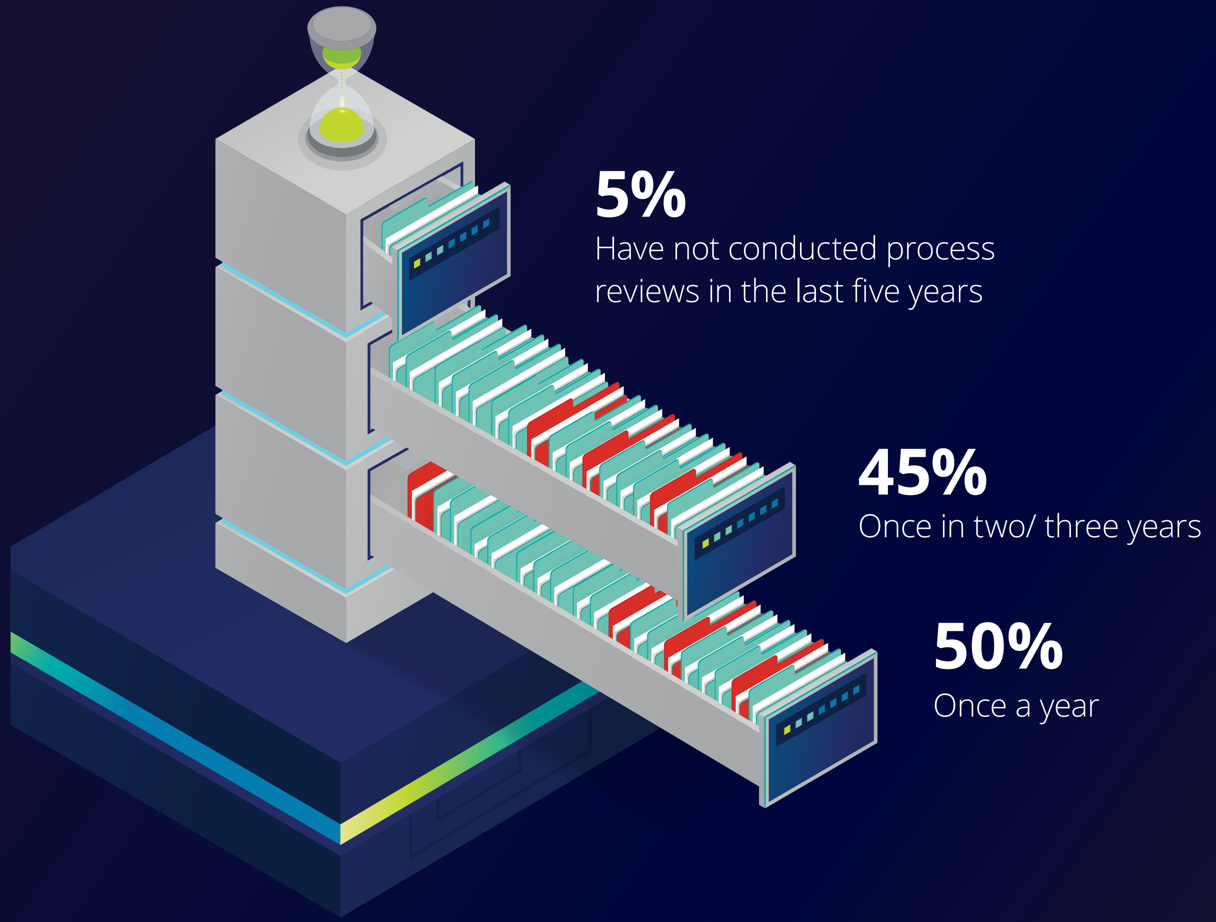
According to 35 and 30 percent respondents, respectively, a fraud incident was detected either during a routine account audit/ reconciliation/process review or through an internal automated data analysis or transaction-monitoring software (EFRMS/EWS). This represents a significant improvement, compared with our previous edition, wherein only 26 and 20 percent respondents respectively attributed fraud detection to the same factors. This also ties in with our experience over the course of the last two years where banks, having realised its effectiveness, have now started using technology, including data analytics to proactively identify frauds.

Which of the following stages in the lifecycle of a MSME/ corporate loan is most vulnerable to fraud?



A majority of the respondents (33 percent) cited end-use monitoring as the most vulnerable stage within the corporate/MSME loan cycle, posing the greatest fraud risk; with sourcing (19 percent) ranked as second. Results of this survey reaffirm the significance and criticality of optimising and ensuring the effectiveness of the post disbursement and continuous monitoring framework. The key to establishing an effective continuous monitoring framework is to get various enablers right, such as an Early Warning System (EWS), market intelligence, and database research, and synchronise their output.

How frequently does your bank conduct fraud risk assessments and update the fraud risk register?



According to the survey findings, 45 percent respondents conduct fraud risk assessments and update the fraud risk registers once in two/three years. Given the dynamic nature of the banking environment, conducting fraud risk assessments every two/three years may not be prudent. Recent years has seen the introduction of new technology enabled products and digital payment channels helping reduce face-to-face touchpoints between banks and their customers. This increased reliance on remote and electronic channels could possibly have given rise to fraud risks that previously may not have warranted as much attention. The change in the banking environment has been compounded by the pandemic-induced disruption, resulting in a greater degree of uncertainty. Conducting fraud risk assessments with greater frequency is an absolute necessity in current times to understand the impact of these changes on fraud, as well as to proactively identify new fraud risks/trends.

What are the challenges faced by your bank while conducting forensic audit in-house?

(Respondents chose all applicable options)

20%	Lack of required skillset to conduct forensic audit
21%	Lack of data analytics capability to evaluate large data set
17%	Absence of a dedicated team or inadequate skilled resources to conduct forensic audit
16%	Inadequate market intelligence capability
26%	Technological limitations to read and analyse Borrower's accounting records maintained in various applications

Top challenges faced by banks in performing a forensic audit in-house include technological limitations to read and analyse the borrower's accounting records (25 percent), lack of data analytics capabilities (21 percent), and lack of requisite skill sets (20 percent). In addition, the lack of a dedicated team, according to 17 percent respondents, is another major impediment. To address these issues, banks should ideally establish a dedicated team to address such requirements and hire external experts to provide necessary training on the necessary skillsets, tools, and technology.

c) Proactive approach in strengthening fraud risk management

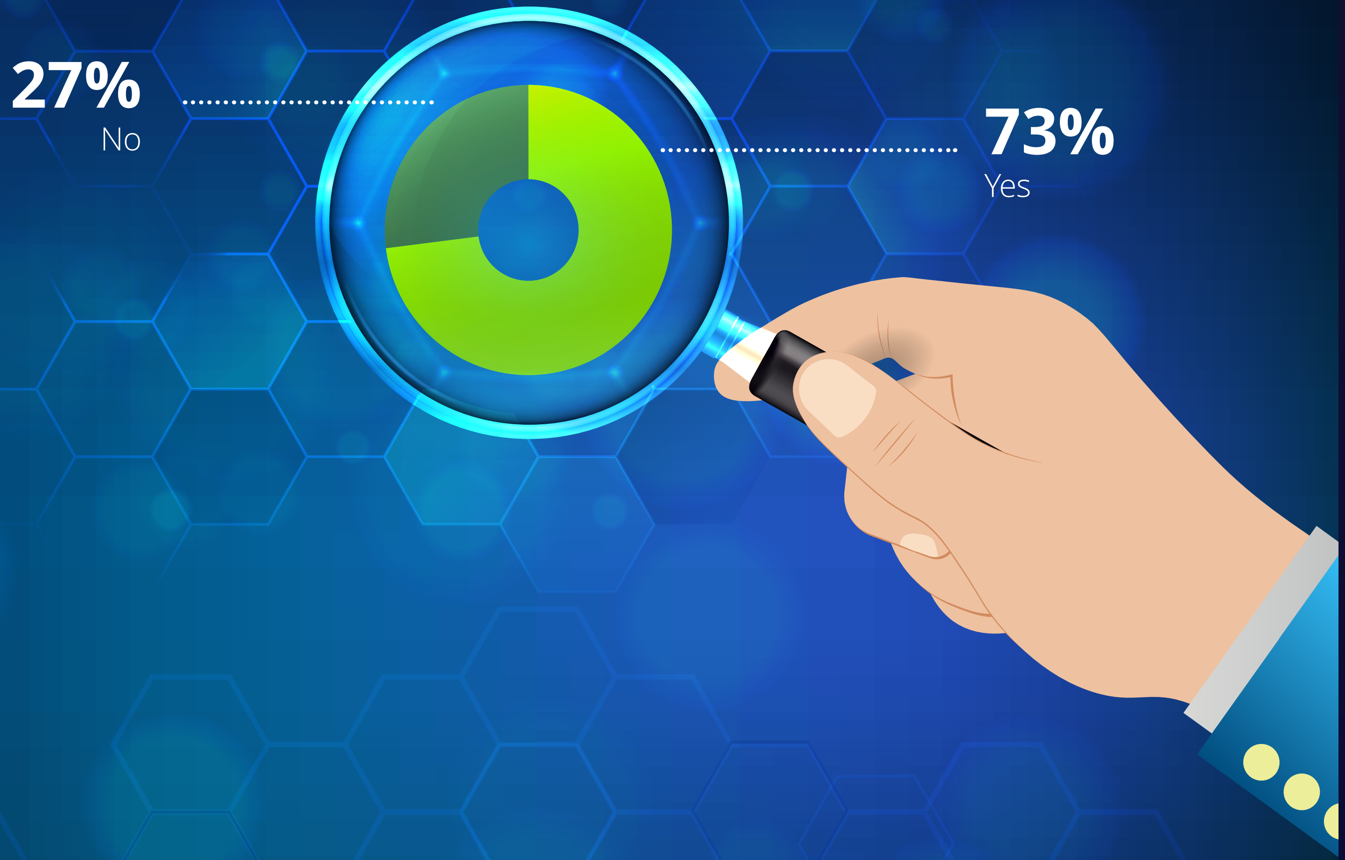
In the last six months, which of the following measures has your bank implemented to mitigate fraud?

17%	Arrange trainings/ workshops to enhance skills of the staff involved in fraud-monitoring functions
16%	Conduct video KYC for customer onboarding, and KYC refresh
13%	E-verify customers' assets/collaterals using GPS or other technologies
13%	Mandate vendors/ customers to use certain software and security measures such as encryption
18%	Enhance Case Management Solutions to effectively respond to fraud incidents, and report on time
23%	Optimise existing EWS and Fraud Monitoring Systems to cater to current banking conditions, using artificial intelligence/machine learning and by integrating external databases

Survey findings reveal that a majority of the investment in fraud mitigation measures has been in optimising existing EWS and fraud monitoring systems using AI/ML (22 percent), enhancing case management solutions to better respond to frauds (17 percent), and providing training/workshops to upskill team members as part of the FRM function (17 percent).

Considering that a majority of respondents indicated end-use monitoring as the most vulnerable stage of the loan lifecycle (to fraud), investments in optimising the monitoring system is to be expected.

Does your bank undertake continuous monitoring of transactions?



As an approach to continuous monitoring of assets, it's encouraging to see that banks have allocated their resources across a combination of methods. This includes 21 percent of respondents relying on a dedicated team with FRM experience to handle high value credits, supported by 15 percent of respondents that highlighted their reliance on data analytics tools such as EWS. Other approaches adopted by survey respondents include a dedicated market intelligence unit attached to the FRM team (12 percent) and use of external sources of information (11 percent). Considering the increase in volume and complexity of transactions enabled by new technologies, the low percentage of respondents opting for data analytics tools for asset monitoring poses a bit of a concern.

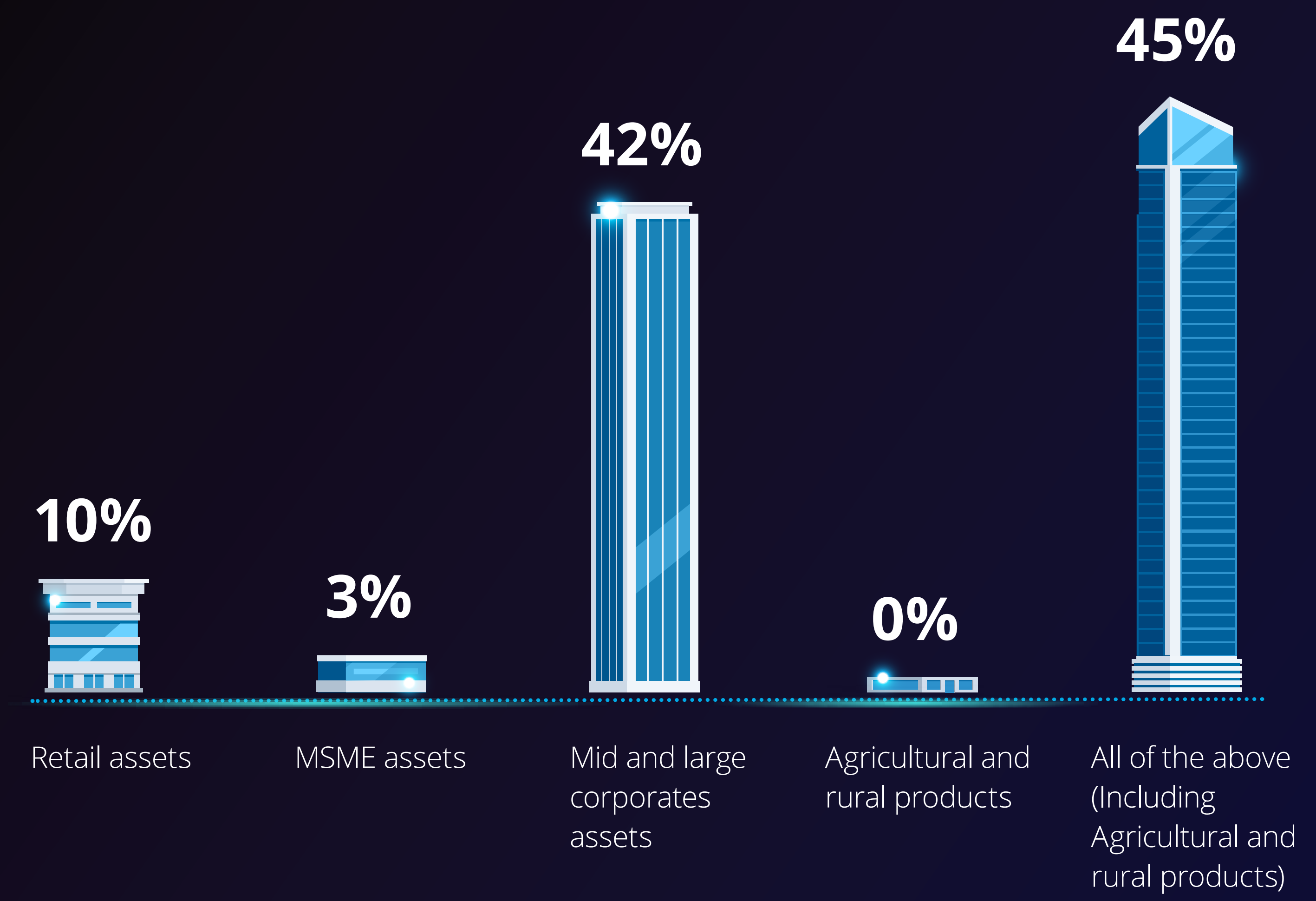
Ideally a continuous monitoring mechanism should include all aforesaid approaches operating in unison for an all-encompassing view of assets. Such a mechanism would aggregate outputs from all the approaches/processes mentioned above, providing more actionable and consolidated intelligence. Reliance on only one or some of these approaches in isolation will not yield effective results.

Which of the following best describes your bank's approach to continuous monitoring of assets?

(Respondents chose all applicable options)

A dedicated team for handling high-value credits staffed by senior employees with relevant experience and skills for FRM	21%
A dedicated Market Intelligence Unit attached to the FRM team	12%
Empanelled vendors/ consultants for conducting market intelligence activities	10%
Use of data analytics tools for monitoring (e.g., EWS, EFRMS)	15%
A dedicated team for evaluating alerts generated	10%
Use of external databases, regulator websites, or other sources to verify information	11%
Tool/Workflow management system to ensure adequate documentation from the customer	8%
Regular process reviews and updates documented in the fraud risk register	8%
End-use monitoring	5%

Which of the following products and assets are included in your bank's continuous monitoring process?



About 51 percent respondents indicated that they do not include MSME assets in their continuous monitoring process, which may be a potential area of concern. To counter the pandemic's disruptive effects, stimulus packages were announced to help support the MSME sector. It is anticipated that the stimulus will lead to a high volume of activity in the sector in new loans and loan extensions. This increase in demand/activity would invariably be accompanied by parties attempting to profit illegally. In this regard, banks should also monitor their MSME assets as part of their ongoing monitoring process.

Section III

Insights | Investing for greater resilience and accelerating efficiency in fraud risk management

Enhancing and complementing FRM teams with market intelligence and data analytics capabilities to ensure continuous monitoring

The Indian banking industry, over the last few years, has emphasised on the significance of establishing anti-fraud cells or fraud monitoring departments to perform investigations and also focus on prevention and the timely detection of potential fraud activities through fraud monitoring systems, etc. However, considering the increasing value and incidents of frauds, as published in RBI's Annual Report for FY 2020-21, there appears to be significant scope to improve the prevention and detection capabilities of fraud monitoring units to make them more comprehensive, and proactive in nature.[2]

In fact, in January 2020, the RBI had provided excerpts of recommendations from the expert committee on NPAs and frauds, constituted under the chairmanship of Shri Y. H. Malegam. The recommendations include setting up a Market Intelligence Unit (MIU) to support fraud risk management, as well as the inclusion of a credit monitoring team in the bank to provide inputs/insights at the time of appraisal/sanctioning/during monitoring of customer activities.

Currently, the alert definitions configured for EWS and fraud monitoring systems are primarily based on a customer's transaction in the bank and financial statements. However, inputs from MIU will help identify and highlight red flags such as the presence of shell companies, feedback from top vendors/customers, reason for change in promoters/management, progress on construction sites, and activity levels in a factory.

To receive timely and relevant results from the MIU, it is important to ensure that the feed provided by the monitoring team to MIU is accurate and current. For example, the feed given to MIU to perform checks on suspicious parties who have received payments from borrowers out of the bank loan should be based on the current information available with the bank. This is where data analytics can play a key role to detect potential fraud cases sooner and reduce financial loss, as opposed to the incident being discovered at a later stage. Data analytics does not only mean configuring pre-defined rules for alert generation but also identifying ever-changing anomalous activity patterns. This dynamism can only be brought about by the use of AI and ML tools.

Over the coming years, banks will need to adopt a more sophisticated approach to fraud risk management by integrating state-of-the-art fraud detection tools, as well as by combining Big Data analytics with AI to generate more meaningful and accurate alerts. Integrating these features with the fraud risk management approach will allow banks/FIs to monitor customers across all stages of their lifecycle, from onboarding to settlement.

[2] https://www.financialexpress.com/industry/banking-finance/rbi-annual-report-number-of-frauds-in-private-banks-up-21-in-fy21/2260406/

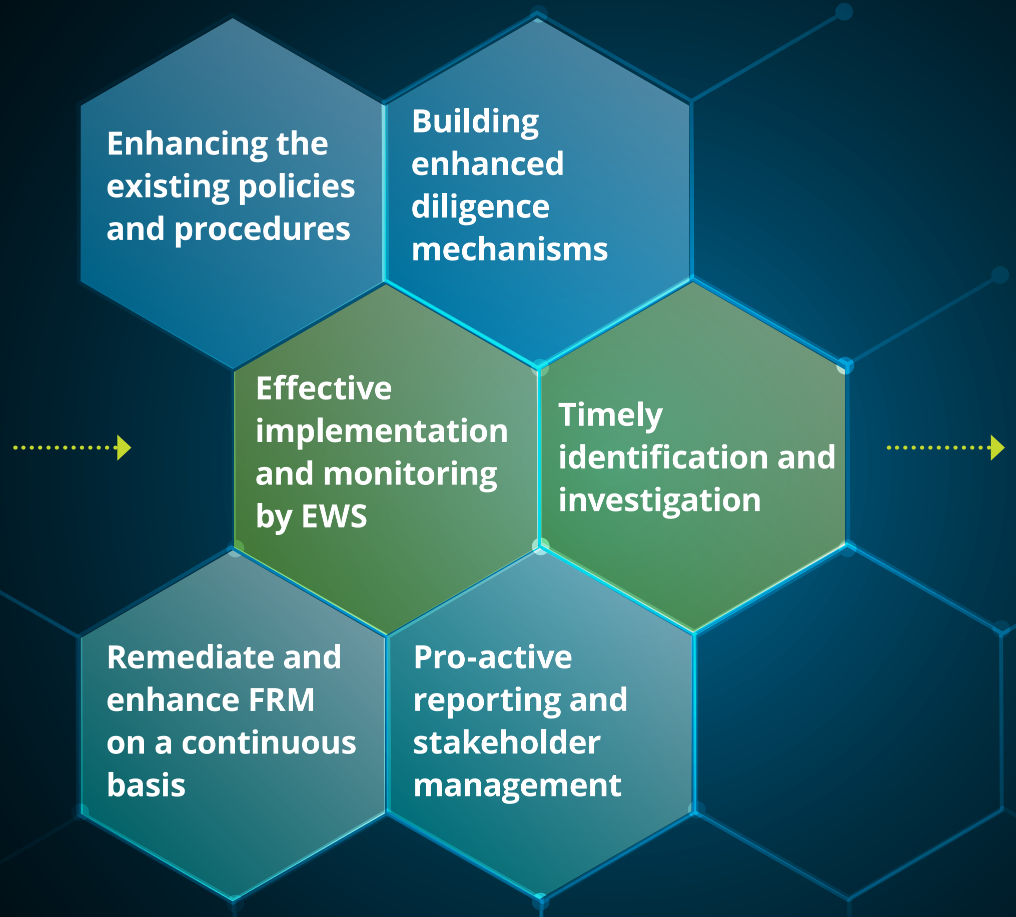
Enhancing the existing FRM function

The current traditional methods of fraud detection are plagued with the lack of centralised control, limited feedback from FRM processes, lack of risk-based monitoring, focus on detection than prevention, etc. To transform to a proactive, agile future and achieve a robust and comprehensive system, EWS and FRM needs to be integrated.

Current state

Traditional and reactive

- **Standalone** anti-fraud/AML policies and procedures
- **Threshold/materiality-**based monitoring of accounts
- **Dependency** on other teams - **Traditional method** of detecting frauds
- **Centralised** training and communication
- More focused on reporting
- **Lack of centralised control** on suspicious cases reported by branches/zones
- Limited feedback from FRM on process and system enhancements
- Lack of risk-based monitoring
- Focus is more on detection than prevention


Enhancing the existing policies and procedures
Building enhanced diligence mechanisms
Effective implementation and monitoring by EWS
Timely identification and investigation
Remediate and enhance FRM on a continuous basis
Pro-active reporting and stakeholder management

Future state

Proactive and agile

Future enhanced FRM

Enhanced due diligence

- Identify anomalies or the potential misrepresentation of facts
- Background checks on promoters/borrowers
- Database screening and source enquiries
- Tweaking of policies and procedures, if any, for the changing environment
- Review asset classification to verify if account showed stress prior to COVID-19 lockdown

Continuous monitoring/ enhanced EWS

- MRI index will provide inputs to design new fraud alert monitoring scenarios
- Identify trigger events to revisit and enrich fraud scenarios
- Optimise EWS with the enhanced scenarios for timely triggers
- Integrate internal and external data sources to identify potential "red flags"

Investigation and remediation

- Conduct thematic testing and portfolio analysis based on MRI
- Detailed investigation including enhanced due diligence, market intelligence, and end use of funds on suspect customers
- Develop additional anti-fraud controls to address identified new risks
- Update and socialise policies/processes
- Robust MIS reporting/ dashboards

Bringing synergy across various fraud risk monitoring tools

Industry-wide banks are using various systems that run pre-defined scenarios and generate alerts, which may be in the form of early warning signals, potential fraud alerts or suspicious alerts, indicating money laundering activities. However, most banks continue to monitor these alerts in isolation.

Several banks have begun to integrate various alert monitoring tools to bring synergy and get a comprehensive view of customers and their transactions. Integration of alerts does not necessarily mean that one team reviews all alerts generated by various tools deployed by banks. Bringing more synergy may entail revisiting the alert scenarios defined in various systems, alignment between the FRM and EWS teams, data sharing between the FRM and credit monitoring/inspection departments to proactively identify red flags, providing meaningful insights to the AML transaction monitoring team for review, and reporting to FIU, if required, etc.

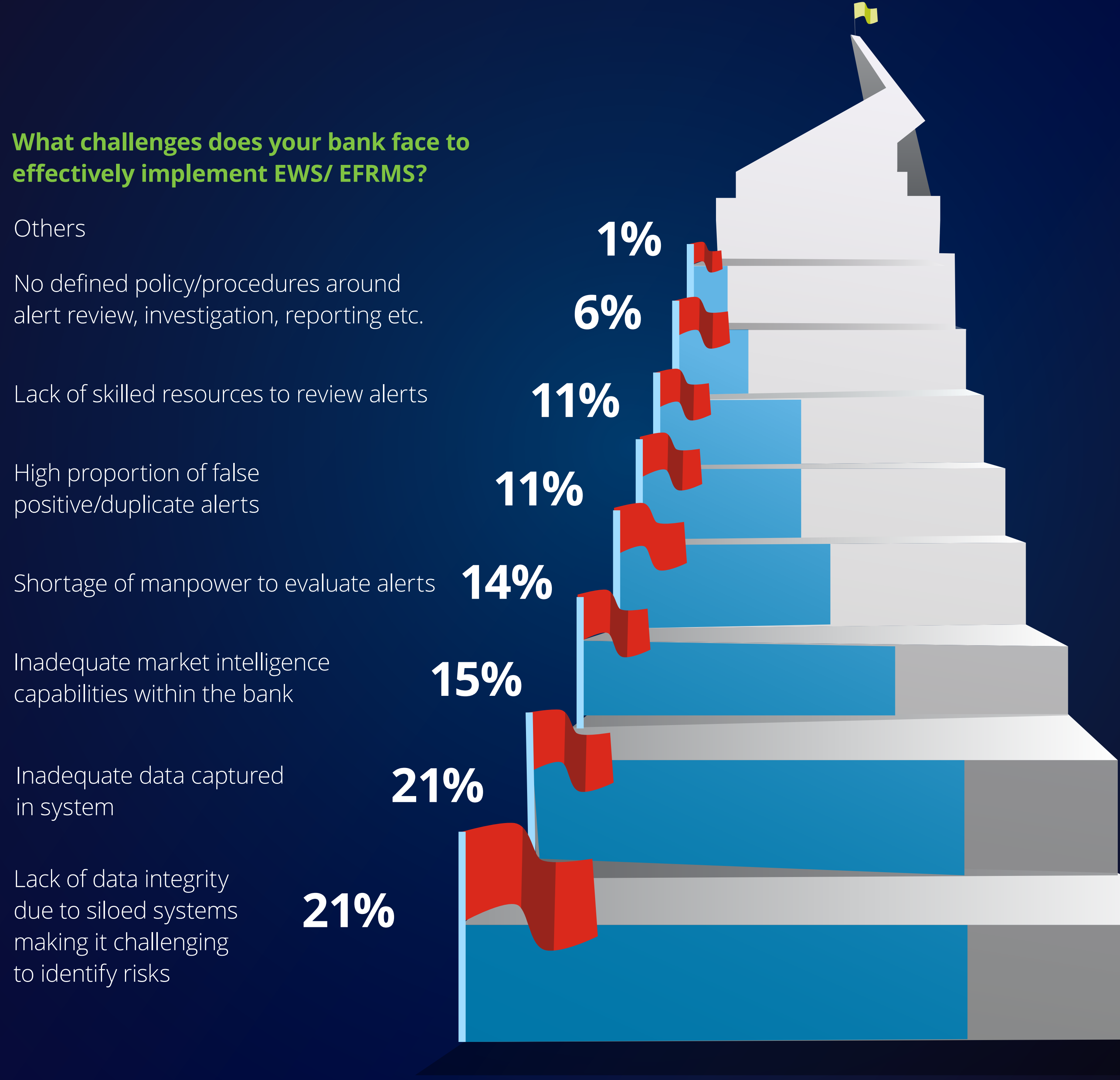
For banks, this combined effort will help achieve the ultimate common objective of protecting its customers from potential financial loss and enhancing trust amongst customers and the banks' stakeholders.

Upscaling resources in FRM

Limited monitoring after disbursement of assets has been identified as a major contributor to stressed assets by more than 38 percent respondents. This appears to have elicited an appropriate response from the banking sector in the form of increased reliance on measures such as EWS and data analytics. The survey also indicates banks' heavy reliance on FRM human resources for effective continuous monitoring of assets, with 20 percent respondents opting for a dedicated team of experienced FRM professionals to handle high-value credits.

The industry seems to have reached a consensus on the need of continuous monitoring and effectiveness of tools, such as EWS and data analytics; however, there appears to be several challenges in the effective implementation of these tools/ measures. The survey cites factors such as lack of data integrity due to siloed systems, lack of dedicated teams and the absence of the overall skill sets required in market intelligence, forensic audits, and EWS alert reviews and analytics, as impediments to operationalise an effective fraud monitoring framework.

What challenges does your bank face to effectively implement EWS/ EFRMS?



The criticality of having an effective fraud monitoring framework has been amplified due to an upward trend in frauds since our previous survey. Concerns are heightened by expectations that the transaction volume will rise as a result of government stimulus and 78 percent survey respondents stating that banking frauds may increase over the next two years. In this regard, upscaling FRM resources is necessary, both in terms of their strength and skill sets. The banking industry needs to identify resources with appropriate skill sets and experience to staff its FRM function and ensure that data analytics capabilities in critical areas such as market intelligence, forensic audits, and EWS alert reviews are developed. This calls upon the banking industry to make strategic investments in areas of training and skill development.

Need to enhance EWS and FRM using AI/ML

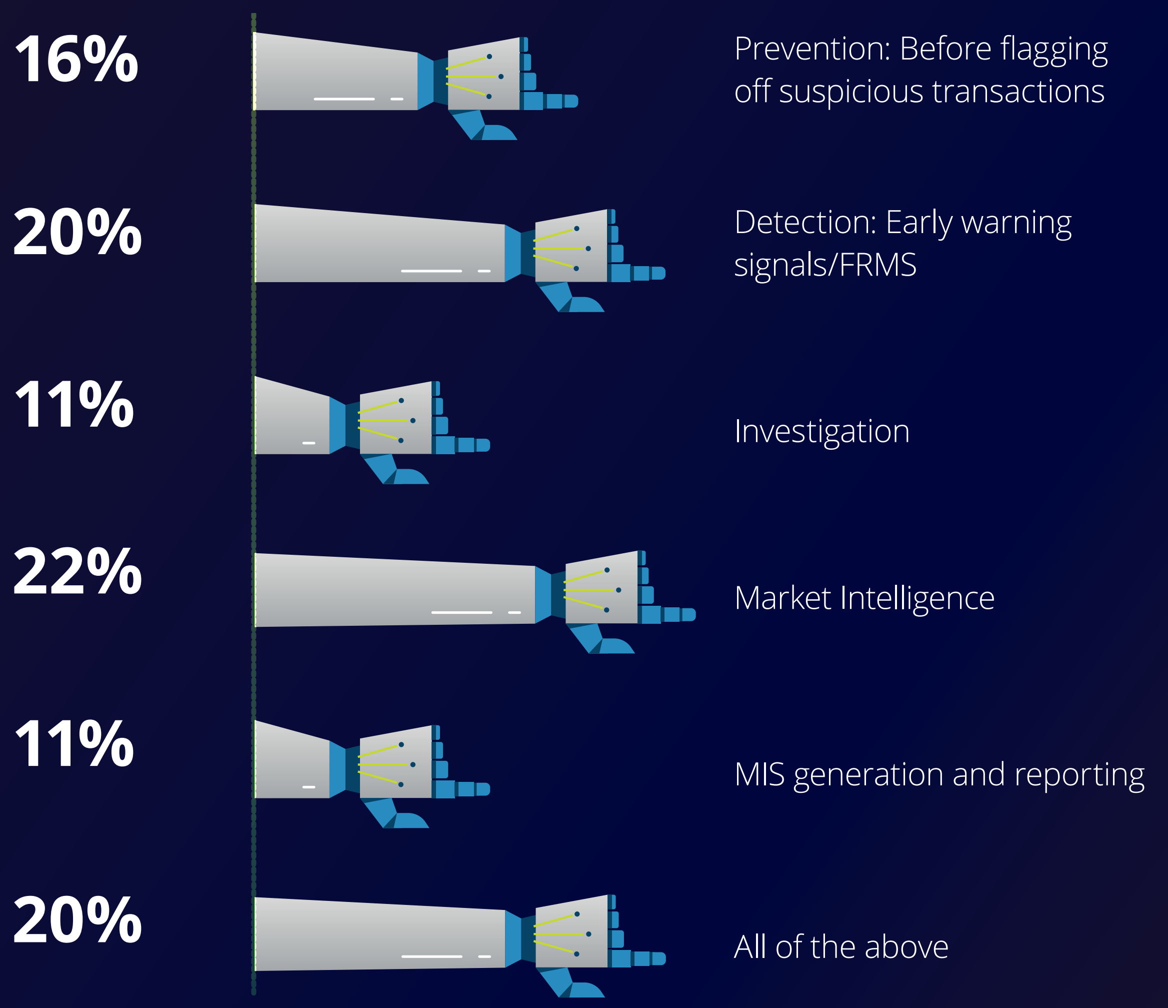
The increase in the use of digital channels for transactions by customers, on one hand, has contributed to the ease and speed of transactions. On the other hand, with evolving business models and increased technology use, fraud risk management frameworks have been introduced to newer and more complex challenges.

This ever-evolving technology across banking channels means that human decision-making and traditional transaction alert systems are no longer effective in the timely detection of frauds.

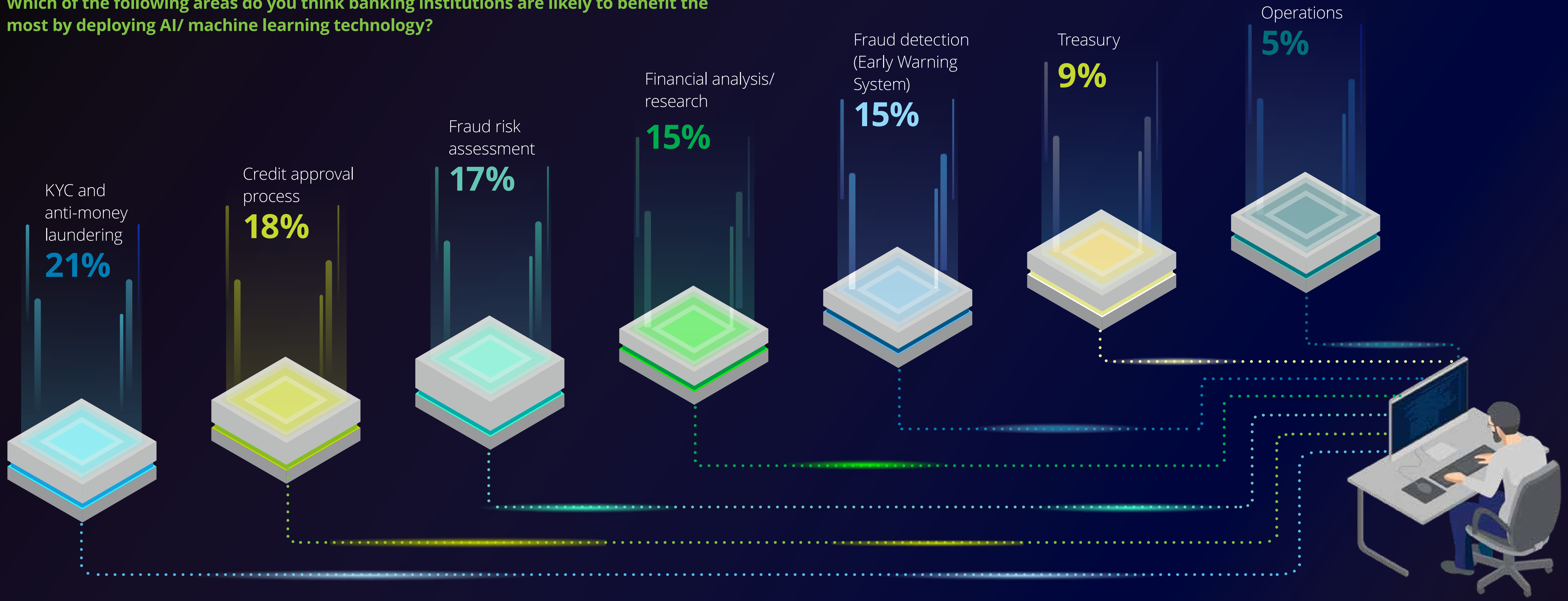
Digitalisation of business transactions has led to an enormous increase in transactions every day, which in turn, has rapidly increased the volume of bank transaction datasets. Interestingly, this data holds several valuable insights that can identify fraudulent behaviour or patterns in the transaction activities of a particular customer at an early stage. An intelligent data analytics tool can mine through vast volumes of data, gather and analyse intelligence from external sources, and identify hidden relationships and red flags. This will enable banks to proactively identify potential fraudulent transactions before they manifest themselves. Through human decision-making, along with machine learning algorithms (that can learn from these datasets), fraud risk identification and detection can be much faster and more efficient.

Currently, most early-warning and transaction monitoring systems that generate fraud alerts are rule-based. When a certain threshold exceeds/certain conditions are met/recurrence is identified, the transaction is marked for further investigation. One operational challenge of such traditional EWS and fraud alert monitoring systems, with predefined thresholds/parameters, is the number of “false positives”—transactions that are flagged as suspicious, but that turn out to be regular. Following up and investigating such false positives can be a very time-consuming and cost-intensive activity for banks. However, by performing periodic reviews of test results and incorporating learnings into monitoring systems, the existing system can learn to detect true anomalies more efficiently, with lower false alarm levels.

In which of the following areas are you currently using Artificial Intelligence and Machine learning tools to improve FRM?



Which of the following areas do you think banking institutions are likely to benefit the most by deploying AI/ machine learning technology?



To obtain better results, AI techniques can be used to reduce false positives and spot true positives and detect new patterns. Anomaly detection algorithms are tailor-made to detect fraudulent transactions by isolating exceptional items based on variables known to the model. The input from risk, compliance, and business teams complemented with intelligence gathered through external sources is essential to implement this use case. In addition, banks can use data segmentation, coupled with statistical analyses to identify characteristics specific to each peer group and create custom thresholds. For example, high net-worth customers tend to be associated with large transaction amounts and may therefore require different parameters than lower income clients. Banks can then perform a sensitivity analysis to help determine whether threshold levels should be increased if too many false alerts are generated or decreased if suspicious activity is being missed, a process known as alert tuning.

There are several benefits to utilising ML in fraud monitoring and detection:

- Works with large datasets – ML is better than humans at processing large datasets and its prediction results improve as datasets grow.
- Reduces operational cost – It eliminates the need to spend as much time and resources on reviewing every alert transaction due to better accuracy and automated predictions.
- Detects and prevents fraud more effectively – ML can quickly adapt to new behaviours of fraudulent transactions and helps improve reactions to suspicious outliers.
- Reduces false positives and prevents frauds with more efficacy.

Advanced analytics can help reshape the way banks conduct fraud tests and monitor their operations. In fact, without using proper data interrogation techniques, efficiently and effectively using all the sources of information available—both internal and external—the process of uncovering fraudulent behaviours may not be as accurate as desired and can take more time and effort, given the large volumes of data generated by banks.

Closing thoughts

The banking business has never been without risk; however, given the current rise in fraud trends, there is an immediate need for banks to implement robust, effective, and efficient control frameworks. Over the past few years, we have witnessed various banks increase their investments in enhancing their FRM frameworks and monitoring systems and controls; however, it appears that these efforts have not been sufficient.

The current siloed approach to fraud risk management will no longer be effective. Whilst banks navigate through these unprecedented times, there are a number of actions that should be considered when protecting their business from fraudsters who want to use the pandemic for their own gain.

1 Review scenarios/rules to reflect the “new normal”. This will ensure banks are neither being inundated by alerts of customers who have deviated significantly in behaviour, such as payment flows being changed significantly due to re-configured supply chains, nor are new patterns/ fraud trends missed out on.

2 With many regulators across the globe releasing guidelines, banks need to take the time to measure the effectiveness, appropriateness, and efficiency of existing controls against an updated risk assessment. Regular/timely and updated risk assessments can help banks ensure that there are linkages between risk typologies and the control framework.

3 Reflect on the technology used/strategy to prevent, monitor, and detect financial crime. A key challenge for banks managing their regulatory obligations is finding the balance between risk management and efficiency/effectiveness through innovation using AI and ML.

The manner in which banks choose to respond to challenges will continue to be the focus of the public, regulators, and investors, and will position them well to cope with any future crises that comes their way.

About the survey

We gathered the views of 70 key C-suite stakeholders/ senior management responsible for compliance and fraud risk management, audit/ finance, asset recovery from varied financial institutions based in India. Banks and financial institutions who participated in the survey included private, public, foreign, co-operative and regional rural banks in India.

Each statistic used in this report is derived from the number of responses to that question and must not be considered consistent across the report. For multiple choice questions and priority-based questions, the weighted average of responses for that question has been used to derive the statistics.

About Deloitte's Forensic practice in India

Deloitte's Forensic practice in India helps organisations protect their brand and reputation through proactive advice on their exposure to fraud, corruption, non-compliance, misconduct, and other future business risk issues. The practice also helps clients react quickly and confidently in a crisis, investigation, or dispute scenario. We use our global network, deep industry experience, and advanced analytical technology to understand and resolve/deal with all such issues. The team comprises of professionals who bring in diverse skill sets to the practice. For more information, you may visit our page.

Connect with us

Nikhil Bedi
Partner and Leader – Forensic
Financial Advisory
Deloitte India
nikhilbedi@deloitte.com

KV Karthik
Partner - Forensic
Financial Advisory
Deloitte India
kvkarthik@deloitte.com

Nishkam Ojha
Partner – Forensic
Financial Advisory
Deloitte India
nojha@deloitte.com

Amol Mhapankar
Director – Forensic
Financial Advisory
Deloitte India
amhapankar@deloitte.com

Soniya Mahajan
Director – Forensic
Financial Advisory
Deloitte India
somahajan@deloitte.com

Manish Mandhyan
Director – Forensic
Financial Advisory
Deloitte India
mmandhyan@deloitte.com

Contributors

Anurag Datta

Soniya Mahajan

Amol Mhapankar

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third-party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. Deloitte, by means of this material, is not rendering any kind of investment, legal or other professional advice or services. You should consult a relevant professional for these kinds of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser. Further, nothing in this material creates any contractual relationship between DTTILLP and you. Any mutually binding legal obligations or rights may only be created between you and DTTILLP upon execution of a legally binding contract.Deloitte shall not be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.