Grant Thornton

#GTBharat
SHAPING VIBRANT INDIA

Financial and Cyber Fraud Report 2024

Revealing fraud vulnerabilities in the post-pandemic era

Contents

Foreword

The trajectory of India's economy has been nothing short of impressive, achieving a commendable growth rate of ~7% over three fiscal years, with projections pointing towards an upward momentum. This positions India as the fastest-growing major economy globally. Amidst this growth and with businesses expanding rapidly, the vulnerability to fraudulent activities has amplified. The COVID-19 pandemic and the subsequent era of post-COVID recovery have significantly altered the landscape of fraud risks in India, especially due to digital transformation.

Recent regulatory changes, such as enforcement of the Digital Personal Data Protection Act, SEBI guidelines on forensic audits, and the NFRA's circular on fraud reporting, have further highlighted the necessity and importance of a robust fraud risk framework and heightened vigilance by corporates.

This heightened regulatory stance, as evidenced by actions taken by entities such as RBI, SEBI and ED in the past year or so, further emphasises the importance of proactive measures.

To comprehensively understand the intricacies of fraud risks in the Indian corporate ecosystem, Grant Thornton Bharat conducted its inaugural Financial and Cyber Fraud Survey. The survey had over 250 CXO respondents from a wide spectrum of sectors, representing different roles and responsibilities, including business and strategy, finance, information technology, risk and compliance, and legal.

Our survey focused on the incidences of fraud in the pandemic and post-pandemic era, their financial impact, the contributing factors, and ways to respond to them. The survey results further provide insights into how Indian organisations have strengthened their fraud risk management practices to safeguard their operations and stakeholders' interests. We hope the findings will help organisations pave the way for informed decision-making and proactive measures to safeguard against fraud risks.

We extend our heartfelt gratitude to the respondents for taking the time to participate in our survey. We look forward to hearing your thoughts on the report.

Dinesh Anand
Partner and Leader,
ESG and Risk Consulting
Grant Thornton Bharat

Executive summary

Key areas of fraud

- Cyber
- Diversion of assets
- Regulatory

Top sectors which faced fraud incidents

- Technology, media and telecommunication
- Financial services
- Manufacturing

Top emerging fraud trends

- Business email compromise
- Social engineering
- Identity theft

This report highlights a sharp increase in fraud during and after the pandemic. One in two organisations surveyed faced instances of fraud, with cybercrime being a large contributor. Large organisations bore significant financial consequences, with 45% reporting a financial impact of INR 1 crore or more due to fraud. India Inc. is now prioritising the adoption of anti-fraud technology and cybersecurity in response because prevention is indeed better than cure.

Vishesh C. Chandiok

Chief Executive Officer
Grant Thornton Bharat

Grant Thornton Bharat's recent Financial and Cyber Fraud Survey uncovers a significant surge in fraud incidents across different sectors. Every second organisation surveyed faced one or more fraud incidents in recent times, with the top three areas of fraud categories being cyber, diversion of assets and regulatory.

The majority of respondents believe there has been a noticeable increase in fraud incidents post the pandemic because of various factors such as the shift from onsite to remote work, lack of internal controls that commensurate with the organisational changes, and technology-related challenges.

In our view, the sentiment expressed highlights a concerning trend as the rapid adoption of technology has outpaced the implementation of adequate governance protocols, leaving organisations more susceptible to cyber fraud incidents across sectors, both in India and globally. A relatively low adoption (~20%) of advanced predictive detection capabilities, such as artificial intelligence (AI) and machine learning (ML) in organisations, further adds to the worry.

Investing in robust governance protocols is crucial for addressing these challenges and mitigating the fraud risks. While most respondents continue to believe that regulatory and enforcement actions are a key driving factor for governance agendas, it is encouraging to note that many organisations are prioritising the adoption of anti-fraud technology and cybersecurity in the strategic agenda of their Board of Directors. This proactive approach recognises the importance of addressing fraud risks and enhancing governance protocols in today's changing risk landscape.

Strengthening governance and compliance frameworks, enhancing awareness training for internal stakeholders and extended ecosystems, and conducting continuous control assessments of high-risk areas are all critical components of a comprehensive anti-fraud and cybersecurity strategy.

The survey underscores multiple aspects of fraud occurrence, focusing on emerging fraud trends, elevating governance through adoption of anti-fraud and cyber security programmes which will enable organisations to build trustworthy businesses.

1 out of 2

organisations surveyed faced one or more instances of fraud

3 out of 4

respondents perceive a significant rise in fraud incidents after the COVID-19 pandemic

3 out of 5

organisations prioritise the adoption of anti-fraud technology and cybersecurity in the strategic agenda of their Board of Directors

In a world increasingly defined by digital transformation, fraud risk evolves in the shadows, necessitating an agile and comprehensive approach to cybersecurity, vigilance and ethical governance.

Deepankar Sanwalka

Senior Partner,
Grant Thornton Bharat

01

The ascent of fraud and its architects

The survey paints a sobering picture – 50% of the surveyed organisations encountered one or more fraud incidents during and after the pandemic, with a substantial majority (77%) of the respondents perceiving a noticeable increase in fraudulent activities due to the COVID-19 pandemic.

Key areas of fraud

- Cyber
- Diversion of assets
- Regulatory

Top three sectors affected by fraud

- **58%** Technology, media and telecommunication
- **51%** Financial services
- **46%** Manufacturing

Following the transformative changes in business operations post-pandemic, cyber fraud and related incidents now account for a significant 64% of all frauds across sectors. The survey reveals that while the shift from onsite to remote work and technology-related challenges are the two key contributors to increased fraud, lack of internal controls also acts as a challenge for businesses across the country.

The survey affirms our broader observation that while the pandemic has accelerated technology adoption, limited investments in governance protocols are a key contributing factor to the increased cyber fraud incidents across sectors. These risks encompass data breaches, ransomware attacks, phishing scams, and advanced persistent threats, which can lead to significant financial losses, operational disruptions, and damage to an organisation's reputation. With the increasing adoption of cloud computing, IoT devices, and AI technologies, the complexity and impact of cyber threats continue to grow.

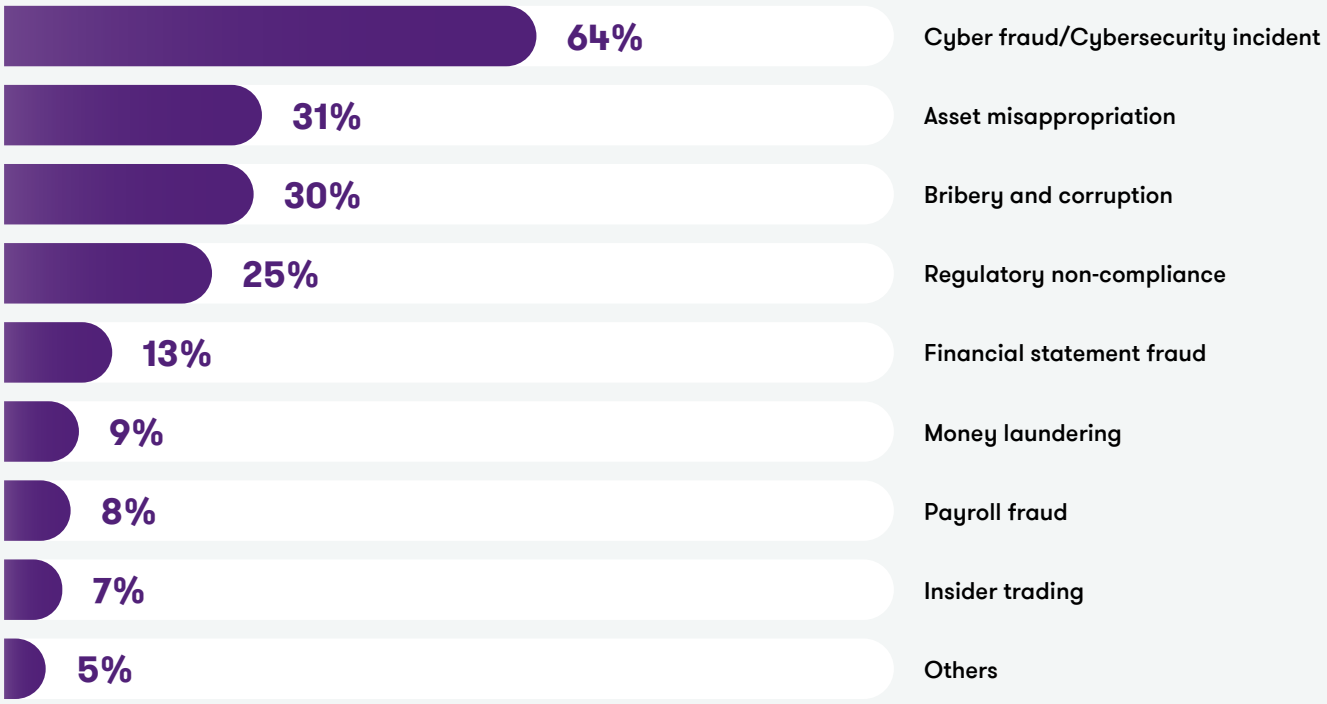
Diversion of assets, commonly known as asset misappropriation, has emerged as another key area of concern basis response of nearly one-third of surveyed organisations. This activity can take many forms, including embezzlement of funds, theft of physical assets, or improper allocation of expenses by employees, management or external parties and concealing those up with 'management' of financial records.

Such activities not only lead to direct financial losses but can also erode trust within the organisation and impair its operational efficiency. Weak internal controls, inadequate monitoring mechanisms and lack of whistleblower protection leading to delayed detection of incidents are the key reasons for continued instances of asset misappropriation. Furthermore, one-eighth of the respondents also faced instances of financial mis-statements. While such instances may be low in absolute numbers, they may have a far more significant impact on organisations and investors leading to monetary, legal and regulatory sanctions.

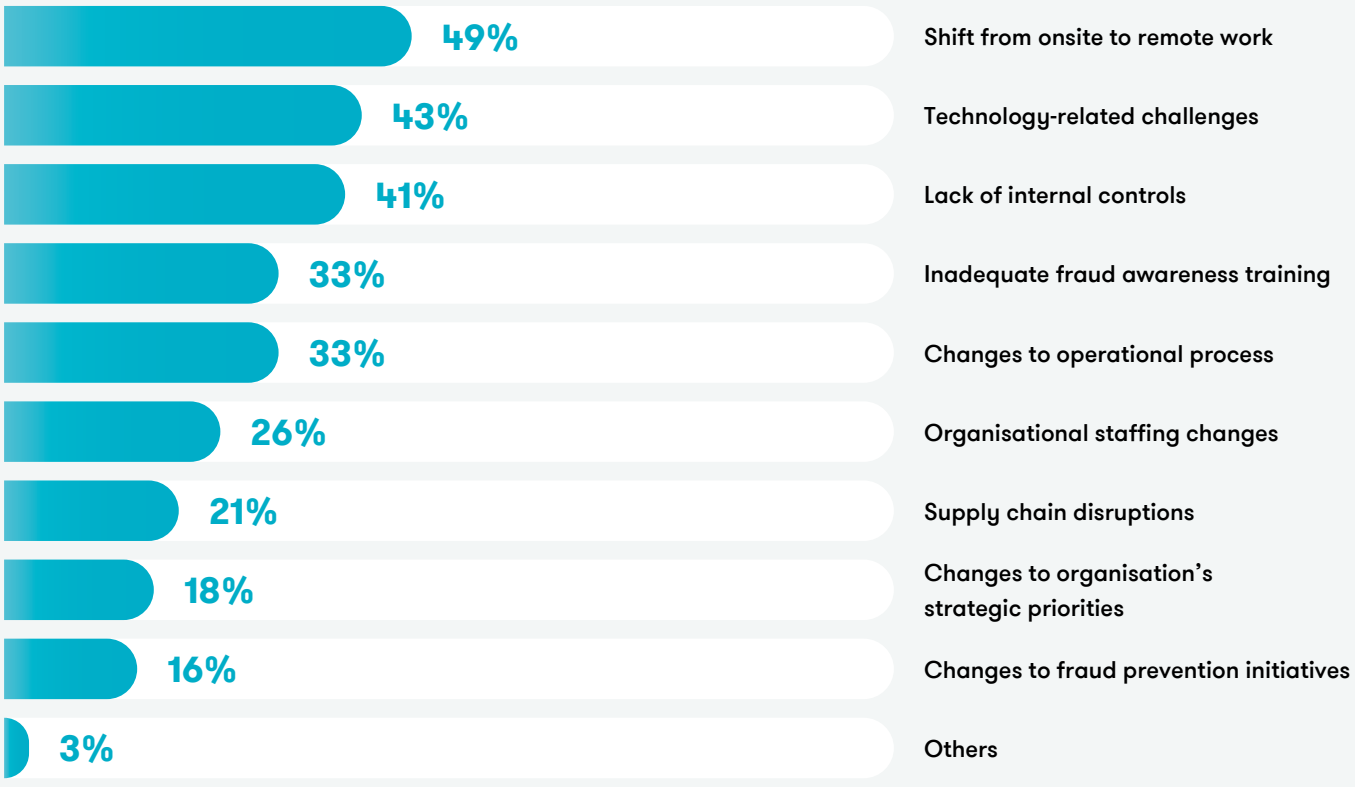
The third biggest area of concern reported is that of regulatory frauds and non-compliance. Bribery and corruption, alongside money laundering, represent severe forms of regulatory fraud that undermine the integrity of India Inc. One-third of the respondents faced bribery and corruption incidents which included instances of employee collusion and kickbacks. The slip in India's ranking in the Global Corruption Perception Index 2023[1] from 85 to 93 further emphasises the need for strong governance controls over bribery and corruption. Regulatory non-compliance was noted to be particularly high in the financial services sector owing to a combination of complex regulations, stringent reporting requirements, heightened risks of financial crime, cross-border operations, and other cultural and demographic factors.

1. Transparency International, Corruption Perception Index 2023

Types of fraud



Factors contributing to increase in fraud



Fraud types by sector

Rapid technological advancements and constant innovation foster growth but create vulnerabilities, as new technologies often outpace the development of adequate controls, leaving loopholes for fraudsters to exploit. This has led to an increase in cyber security incidents across sectors.

In the manufacturing sector, a large volume of inventory and physical assets increase the risk of theft, misuse of company equipment, or fraudulent manipulation of inventory records. Conversely, technology and media companies, which heavily rely on digital platforms and software, may face the risk of intellectual property leakage due to asset misappropriation.

Companies in the TMT and manufacturing sectors typically operate within complex supply chains that often span multiple countries and involve numerous parties. These environments create opportunities for bribery and corruption, including procurement fraud, conflicts between vendors and employees, kickbacks, and more. The intricate networks and layers of subcontractors and suppliers can obscure accountability and make oversight challenging. In such settings, illicit practices may arise as businesses seek to navigate systems or secure contracts and permits in regions where corruption is endemic.

Top 3 fraud risks by sector

Technology, media, and telecommunications

63%	Cyber fraud/Cyber security incident
42%	Asset misappropriation
26%	Bribery and corruption

Financial services

66%	Cyber fraud/Cyber security incident
31%	Regulatory non-compliance
28%	Financial statement fraud

Manufacturing*

75%	Cyber fraud/Cyber security incident
41%	Bribery and corruption
38%	Asset misappropriation

Pharma and healthcare

60%	Cyber fraud/Cyber security incident
20%	Regulatory non-compliance
20%	Financial statement fraud

Real estate and infra

40%	Cyber fraud/Cyber security incident
40%	Bribery and corruption
20%	Other

* Includes consumer and retail, manufacturing and industrial products, auto and auto components

Unveiling the ripple effect

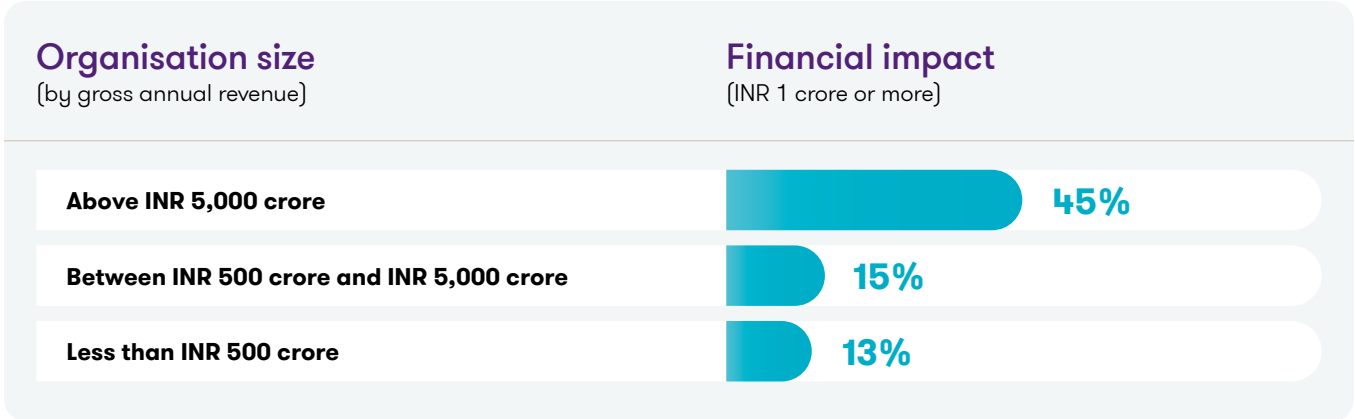
Exploring the impact of financial fraud

One-fourth of the respondents faced financial fraud of **INR 1 crore** and above. Out of these, three-fourth faced an impact of **INR 5 crore** and above.

Correlation between organisational size and financial impact of fraud incidents

Fraud incidents are not arbitrary; financial impact has a clear correlation with an organisation's size, measured by gross annual revenue. The survey shows that larger organisations bear more significant financial consequences from these incidents. The same trend was noted for organisations with private equity investments (PE portfolio companies), where one-third of the investee companies experienced a financial loss of over INR 1 crore or more.

Our survey revealed that the top three types of fraud experienced by organisations with an annual revenue exceeding INR 500 crore closely matched the overall distribution of fraud types. However, our findings suggest that organisations with gross annual revenue below INR 500 crore tend to face regulatory non-compliance as the primary type of fraud, alongside cyber fraud and asset misappropriation. This trend could be attributed to various factors, such as resource limitations, a focus on business growth and operational efficiency at the expense of governance and compliance, inadequate policies and procedures, and the absence of a strong governance framework.

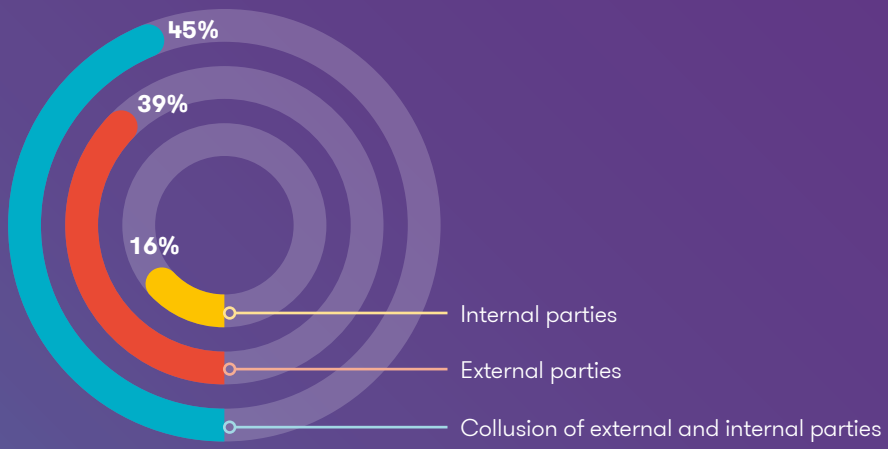


Role of internal and external perpetrators

Fraud perpetrated through internal or external stakeholders poses a significant threat to organisations across sectors. The survey reveals that **84%** of organisations experiencing fraud noted the role of an external perpetrator either standalone or colluding with individuals within the organisation.

A coordinated effort between external and internal parties, such as vendors, customers, or other entities interacting with the organisation, represents a complex and insidious threat to organisations. Frauds involving collusion may include sharing insider information, bypassing security measures, and manipulating organisational processes for mutual financial gain or coercion.

Collaborative nature of fraud



PE portfolio companies mirror this trend, with half of reported frauds involving a partnership between internal employees and external perpetrators. Notably, collusion is prevalent across various sectors, with the financial services sector being an exception; 55% of the respondents perceived external parties such as vendors, customers, and other entities transacting with the organisation as the primary wrongdoers.

In our view, the change in the fraud risk landscape will challenge the traditional fraud-prevention measures undertaken by organisations and become an impetus for change in the anti-fraud and cyber security prevention strategy of India Inc.

Collusion between external and internal factions creates a breeding ground for corruption, where ethical boundaries blur and pillars of integrity and accountability corrode.

02
Emerging fraud trends

While companies continue to combat traditional frauds, new-age digital frauds pose a significant threat to Indian corporates. Our survey highlights that business email compromise (BEC), social engineering, and identity theft are the leading emerging fraud threats in the current landscape.

BEC, wherein fraudsters use compromised or spoofed email accounts to deceive individuals into making fraudulent payments or disclosing sensitive information, ranks among the most prevalent frauds in the current landscape. This organised form of cybercrime can be executed through spoofed domains or via social engineering tactics. Impersonating CEOs and/or employees of an organisation has become one of the most recognised forms of BEC in India.

Social engineering and identity theft, whereby fraudsters manipulate individuals to divulge or wrongfully obtain their personal confidential information, consistently rank high across sectors. This highlights the vulnerability of being duped and the low levels of awareness amongst individuals and employees. Traditional cyber fraud techniques exploit technical vulnerabilities, whereas social engineering and identity theft use psychological tactics to gain an unfair advantage. Deepfake, where fraudsters digitally alter media to impersonate individuals or create misleading content, has emerged as another leading form of cyber fraud.

New-age frauds, such as ransomware attacks, may require negotiations, which is a complex area and requires expertise to manage such conversations. Coordination with regulators and recovery of funds are of critical importance in case of cyber incidents, particularly as some of these matters may become multi-jurisdictional.

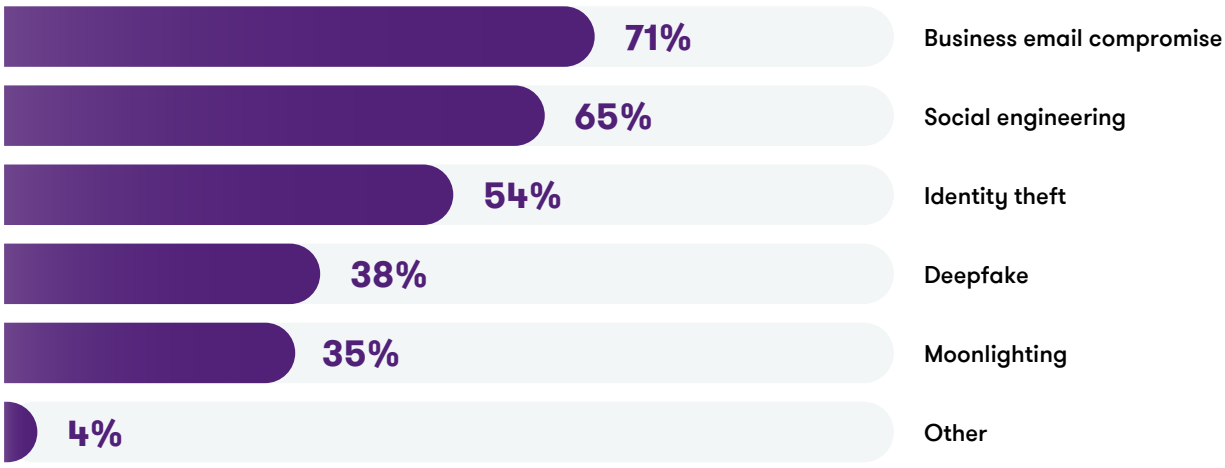
As digital innovation accelerates, so does the complexity of fraud risks, introducing a spectrum of new and emerging threats that challenge traditional safeguards and demand a proactive, adaptive approach to cybersecurity and fraud prevention.

Samir Paranjpe
Partner - Forensic,
Grant Thornton Bharat

It is also interesting to note that for more than one-third of the respondents, moonlighting appears as a key emerging fraud trend. Moonlighting is not a new practice, but the technology industry continues to see an upsurge due to recent changes in working models, such as hybrid working or work from anywhere.

Considering these threats, organisations should prioritise measures to safeguard company data through enhanced data protection and cybersecurity protocols. This may include implementing robust authentication measures, conducting regular security awareness training, and employing advanced technology solutions to detect and prevent fraudulent activities.

Emerging threats



03

Securing integrity

Implementing anti-fraud and cybersecurity programme

Proactive strategies

Organisations, especially larger ones, are increasingly adopting anti-fraud technology and cybersecurity, showcasing a positive correlation between revenue and the integration of these measures into strategic plans. Of the organisations using anti-fraud and cyber security related tools and technologies, 52% observed a decline in fraud. In line with this, 60% of organisations have made adopting anti-fraud technology and cybersecurity a strategic priority for their Board of Directors.

Over one-third of the respondent organisations were uncertain if their anti-fraud and cybersecurity programmes had successfully reduced fraud incidents, signaling an opportunity for a more multifaceted approach. This approach could include the development and communication of various indicators and metrics to raise awareness and effectiveness, such as establishing key performance indicators focused on fraud prevention and detection, implementing robust controls, regularly monitoring and analysing fraud trends, and conducting both internal and external reviews.

Observed a decline in fraud

52%

Not aware whether there is a decline or not

39%

Have not seen a decline

9%

Reactive fraud countermeasures

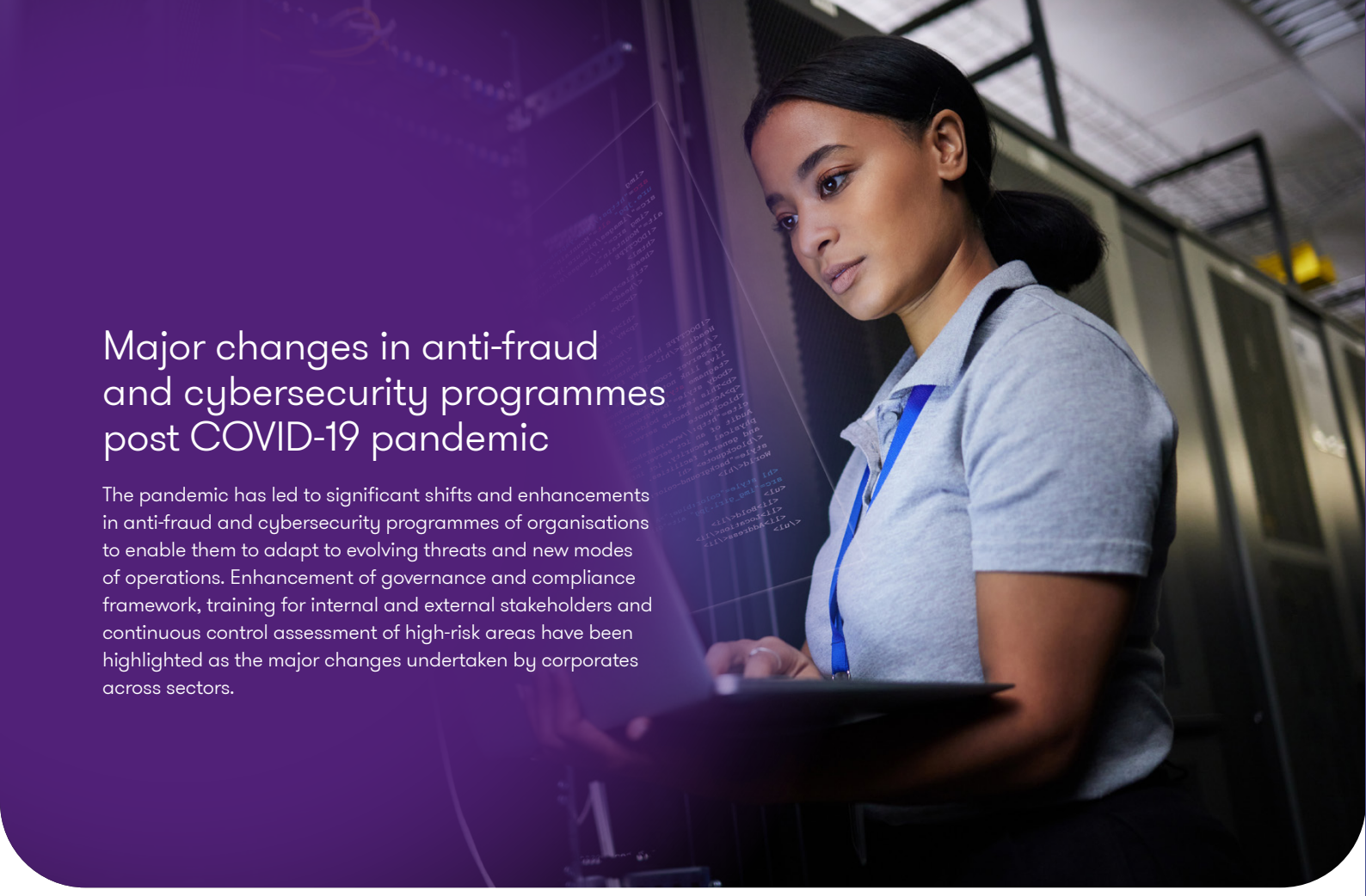
Investigation of fraud is a complex activity that requires corroboration of facts noted through multiple sources both within and outside the organisation. One of the pivotal aspects of the investigation process is data discovery, which involves collection and review of relevant information for uncovering the facts. In addition to conducting an internal inquiry, companies engage external forensic professionals who bring in expertise and objectivity to the process.

Further, under the recent Digital Personal Data Protection Act, 2023, companies need to maintain the privacy and security of personally identifiable information throughout the data discovery process. By leveraging skills of forensic professionals, organisations may also be able to ensure that the investigation is conducted in accordance with legal requirements and that personally identifiable information is handled and protected appropriately.

Our survey shows that 63% of the organisations support a collaborative approach with external forensic professionals to investigate fraud in order to make the fact-finding process more thorough and effective.

In the relentless pursuit of integrity, investigating fraud and implementing comprehensive anti-fraud and cybersecurity programmes are not just strategic defenses but essential keystones for protecting and enhancing organisational trust.

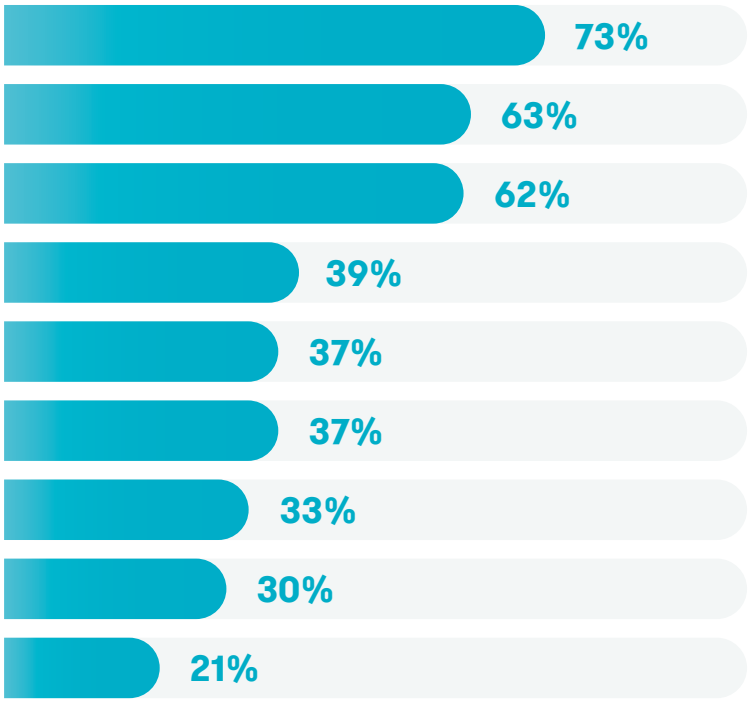
Rahul Lalit
Partner - Forensic,
Grant Thornton Bharat



Major changes in anti-fraud and cybersecurity programmes post COVID-19 pandemic

The pandemic has led to significant shifts and enhancements in anti-fraud and cybersecurity programmes of organisations to enable them to adapt to evolving threats and new modes of operations. Enhancement of governance and compliance framework, training for internal and external stakeholders and continuous control assessment of high-risk areas have been highlighted as the major changes undertaken by corporates across sectors.

Major changes made



- Enhancement of governance and compliance framework
- Enhanced awareness trainings to employees, third-parties and customers
- Continuous control assessment of high-risk areas at regular intervals
- Strengthened whistle-blower/vigil mechanism
- Higher investment in forensic and cybersecurity tools and technologies
- Increased third-party due diligence
- Enhanced employee background checks
- Implemented crisis response planning and emergency response teams
- Embedded predictive detection capabilities such as AI and ML

Additionally, the survey also noted that over 80% of organisations are planning significant or moderate investments in cybersecurity measures over the next three years. These trends closely correlate with the revenue and size of the organisation's workforce, indicating that larger companies are more inclined to prioritise and invest in cybersecurity.

TMT and financial services stand out as leading sectors that consistently prioritise cybersecurity assessments and audits. The survey sheds light on a concerning disparity in the adoption of cybersecurity practices amongst traditional sectors such as manufacturing, real estate and infrastructure. These sectors have historically focused more on operational efficiency rather than digital security, resulting in a slower integration of cybersecurity measures, leaving them more vulnerable to risks.

Interestingly, in response to the increasing shift towards digital business processes, approximately 77% of organisations across various sizes and sectors are turning to external vendors for their IT and cybersecurity needs. This trend reflects a growing demand for specialised services and technologies to drive competitiveness, further fuelling the growth of third-party vendors. Ultimately, this expansion is key to enhancing efficiency, fostering innovation, and increasing flexibility within organisations.

However, despite a positive trend in the adoption of anti-fraud and cyber security programmes, only one-fifth of respondents have incorporated advanced predictive detection capabilities, such as AI and ML, into their anti-fraud and cybersecurity initiatives. This could be due to several key factors such as:

- Complexity in implementing AI and ML solutions and lack of in-house expertise needed to effectively implement these solutions
- Cost of initial setup in AI and ML systems, which can be substantial
- Data challenges and integration issues arise because of incompatibility between legacy systems and newer technologies, which may initially produce false positive and false negative results
- Cultural resistance due to fear of change, concerns about job displacement, or a lack of understanding of the potential benefits
- Regulatory and ethical considerations, such as the use and processing of personal data, which can slow down the adoption of these technologies

With careful planning, the right talent development and a clear focus on addressing ethical, regulatory and operational concerns, some of the above challenges can be overcome. The relatively low adoption rate of predictive capabilities presents an opportunity for organisations to explore and invest in cutting-edge technologies, which will only become imperative in the near future.

Cyber risk is pervasive across industries, prompting regulators to a higher vigil for public interest, national security and digital ecosystem integrity. This calls for cyber readiness, board assurance, brand protection, stakeholder awareness, continuous vigilance, reliance on third-party ecosystems and ongoing compliance for adherence to data privacy regulations.

Akshay Garkel
Partner and Leader - Cyber, Grant Thornton Bharat

04

Elevating governance

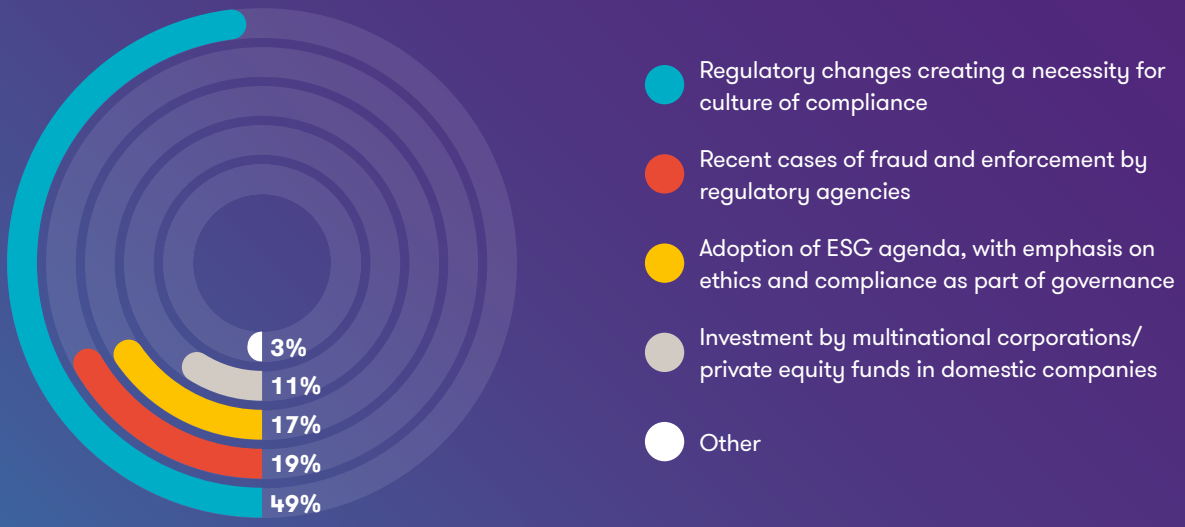
Key driving forces

The survey results underscore the undeniable influence of regulatory dynamics, with a significant **68% of the respondents pointing to regulatory changes and enforcement actions** as the primary force driving the establishment of governance and cybersecurity protocols.

The above trend is especially noticeable in public sector, financial services, and manufacturing, where regulatory frameworks are continually changing or developing. In such sectors, organisations are required to refine their approaches to governance and cybersecurity for sustained compliance. This underlines that a culture of compliance is not merely a best practice but an essential survival strategy.

Adoption of the ESG agenda as one of the top three critical factors pushing governance and cyber security indicates that ESG considerations are gaining traction amongst organisations. This reflects a broader recognition of the importance of ethical considerations in organisational decision-making and risk management strategies. Aligning with societal expectations, integrating ESG principles into governance frameworks enhances long-term sustainability and resilience.

Most critical factors pushing governance and cybersecurity requirements in corporate world



Elevating governance is crucial for businesses for several reasons:

- Governance practices lead to transparency, accountability and integrity, which in turn provides enhanced investor confidence.
- Businesses with elevated governance standards are better positioned to access capital markets and raise funds. Stakeholder interests are better protected with effective governance mechanisms.
- Governance practices ensure compliance with regulatory requirements, essential to avoid legal implications.
- Strong governance frameworks enable businesses to identify, assess, and mitigate risks in a timely and effective manner.
- By prioritising governance, Indian businesses can strengthen their foundations, foster trust, and create value for all stakeholders in the long run.

The Audit Committees and Board of Directors, including active participation of Independent Directors, play a pivotal role in enhancing governance frameworks in an organisation with their expertise, guidance and oversight. By cultivating a diverse board composition, organisations are enhancing their governance structures, promoting transparency and accountability.

Embracing tailored solutions in line with the requirements of the entity can help address compliance challenges effectively. Utilising advanced technologies allows organisations to enhance their governance frameworks while continuing to focus on building internal controls, creating awareness amongst employees, and developing the required frameworks. This proactive approach helps mitigate risks and promotes trust, resilience and long-term sustainability within the organisation.

Acknowledgements

For further information about this report, contact:

Dinesh Anand
Partner and Leader - ESG and Risk Consulting
Grant Thornton Bharat
E: dinesh.anand@in.gt.com

Akshay Garkel
Partner and Leader - Cyber
Grant Thornton Bharat
E: akshay.garkel@in.gt.com

Rahul Lalit
Partner - Forensic
Grant Thornton Bharat
E: rahul.lalit@in.gt.com

Samir Paranjpe
Partner - Forensic
Grant Thornton Bharat
E: samir.paranjpe@in.gt.com

Contributors

Ishan Mahajan
Director
Grant Thornton Bharat

Ankita Lalchandani
Associate Director
Grant Thornton Bharat

Palak Maheshwari
Associate Director
Grant Thornton Bharat

Devangini Mitra
Manager
Grant Thornton Bharat

Achintya Seshadrinathan
Manager
Grant Thornton Bharat

Kajal Gupta
Assistant Manager
Grant Thornton Bharat

Editorial review

Shabana Hussain
Akshay Kapoor
Dhriti Sharan

Design

Vikas Kushwaha

For media enquiries, write to

media@in.gt.com

Great Place To Work® Certified DEC 2023 – DEC 2024 INDIA ™

Best Workplaces™ in Professional Services
Great Place To Work® INDIA 2023

We are
Shaping Vibrant Bharat

A member of Grant Thornton International Ltd., Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more **#VibrantBharat.**

Our offices in India

Ahmedabad • Bengaluru • Chandigarh • Chennai
Dehradun • Delhi • Goa • Gurgaon • Hyderabad
Kochi • Kolkata • Mumbai • Noida • Pune

Scan QR code to see our office addresses
www.grantthornton.in

Connect with us on

@Grant-Thornton-Bharat-LLP
@GrantThorntonBharat
@GrantThornton_Bharat
@GrantThorntonIN
@GrantThorntonBharatLLP
GTBharat@in.gt.com

5624 | SH | VK