Deloitte.

Middle East Fraud Survey

2021

Contents

About the survey

We are pleased to present the 2021 Deloitte Middle East Fraud Survey. 105 anonymous respondents across a spectrum of industries in both the public and private sector participated in the digital questionnaire. The survey consisted of 31 questions relating to the following topics:

- The extent and various types of fraud faced by organisations in the region.
- The impact of the global pandemic on fraud risk due to changes in the business environment.
- Measures being taken to prevent, detect and respond to fraud.

The majority of respondents represented senior management within their organisations, with over half comprising Board Members, Chief Executives, and Chief Operations Officers. They represented various industries such as Financial Services, Real Estate and Infrastructure, Technology, Media and Telecom, Luxury Products, Automotive and Professional Services.

Introduction

This fraud survey illustrates how organisations across the Middle East have been affected by fraud, and their response during the recent COVID-19 pandemic. The survey covers the types of financial and non-financial frauds along with the impact, the company response when faced with a fraud-related incident and measures that organisations have taken to mitigate the fraud risks.

The survey indicates that 48% of participants have witnessed more fraudulent incidents this year as compared to earlier years, and 35% felt it has increased since the start of the COVID-19 pandemic. The top factors in the current business environment contributing to fraud were identified as dependency on technology and remote working.

When comparing these findings to a similar survey conducted by Deloitte Middle East in 2010, it is interesting to note that there has been a change in the most prevalent types of fraud over the last decade; theft of physical assets and misuse of information were the most pressing concerns in 2010 compared to the threat of new age technology frauds such as cyber crime and financial misreporting today. More than two-thirds of the respondents feel that the current business and economic disruptions could increase fraud risk in their organisation over the next two years.

59% of the Companies have a basic policy-level fraud risk framework comprising components such as anti-fraud policy, code of conduct and anti bribery and corruption policy. However, they lacked other necessary elements of the fraud risk framework such as regular trainings, senior management reporting, periodic fraud risk assessment and dedicated anti-fraud technologies for ongoing monitoring of potential frauds.

41% of the companies do not have a dedicated fraud risk management and investigation team and feel that the current fraud risk framework is not adequate to prevent and mitigate the risk of future fraud. Furthermore, the respondents indicated that their employees are not aware of risks pertaining to their industry and the best practices to be followed.

We observed an increase in the percentage of companies with an existing whistleblower policy from 50% to 75% over the past decade. However, over 33% of the respondents stated that the whistleblowing facility was either ineffective or were indifferent about its effectiveness.

Fraud risk assessment and fraud related trainings form an essential part of a fraud prevention framework. Close to two-thirds of organisations in the Middle East have conducted fraud risk assessments and fraud related trainings in the past, however, almost half of the respondents felt the fraud risk assessment conducted was ineffective.

Key elements of anti-fraud management

Based on the information from the results of the survey, and leading guidance from the Association of Certified Fraud Examiners (ACFE), the following have been identified as key elements of an effective fraud risk management framework:

Anti-fraud culture: the promotion of an anti-fraud tone and culture by leadership is a key pillar of every fraud risk management framework.

Past fraud analysis: an effective fraud risk management programme takes learnings from past fraud incidents to fine-tune the framework and prevent similar frauds from occurring in the future.

Proactive fraud risk assessment: periodic assessment and review of the likelihood and impact of different fraud scenarios along with an assessment of the organisation's preparedness against such fraud risk should be the foundation of risk mitigation.

Continuous monitoring: the use of tools and technology for real time/ near real time ongoing monitoring of the potential fraud risks is critical to prevent fraud incidents in the future.

Whistleblowing: a whistleblowing policy that ensures no retaliation occurs against the reporter, and an efficient whistleblowing mechanism is vital to detect fraud early on.

Investigations: established procedures for the investigation of suspected frauds must be in place to ensure a transparent and effective investigation.

Key fraud risks and contributing factors

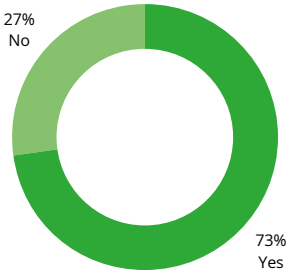
The COVID-19 pandemic has disrupted businesses and economies across the globe and has exposed significant fraud-related vulnerabilities. Over 35% of respondents said that there has been an upward trend in fraud within or against their organisation since the start of pandemic. The evolving nature of the pandemic has revealed that the intervention of technology and remote working are contributing factors towards fraud risk. This was supported by the survey which revealed that cyber and technology-related fraud have been the biggest threat for organisations in the last two years.

Compared to our previous fraud survey conducted in 2010 where the procurement process was considered to be the most vulnerable, today's survey reaffirms that it continues to be an area of concern as the majority of fraud is most likely to be perpetrated in this area. This also indicates that the risk of fraud is more likely to increase with the involvement of external parties.

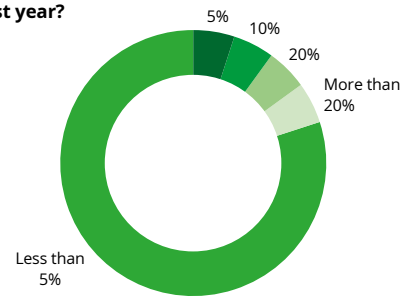
It is recommended that companies review their cyber resilience, business continuity, and procurement policies to include controls which are reflective of the evolving fraud risk landscape.

Changes to business operations have led to two-thirds of the respondents believing that the current business and economic disruptions could significantly increase fraud risk over the next two years. We predict that fraud incidents will continue to grow due to the changes in the overall business environment, when taking into consideration respondents' concerns about their controls environment ineffectiveness.

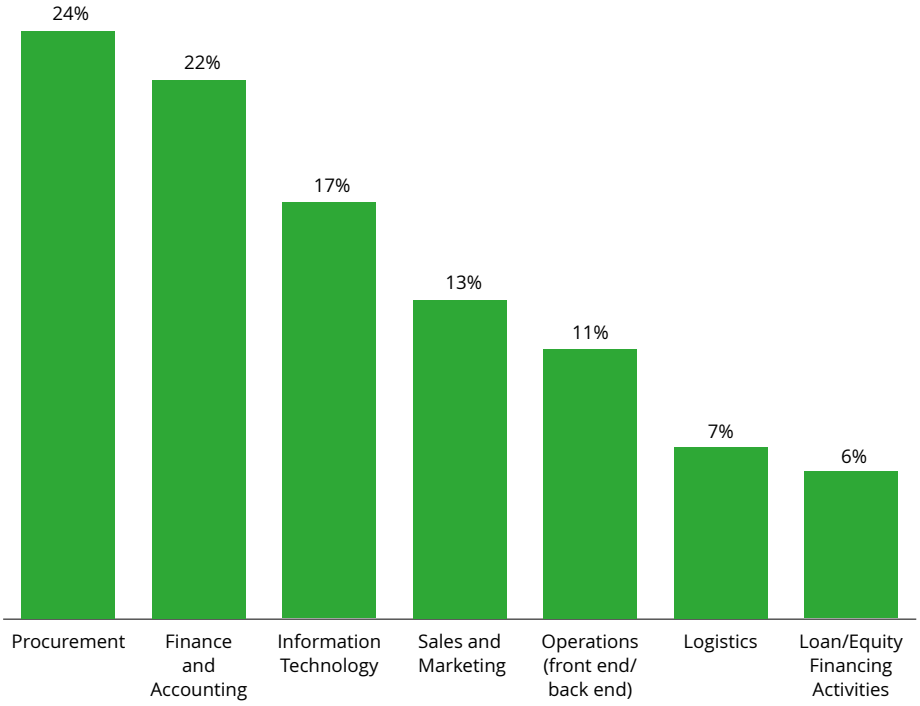
Do you believe that the current business and economic disruptions could increase fraud risk in your organisation over the next two years?



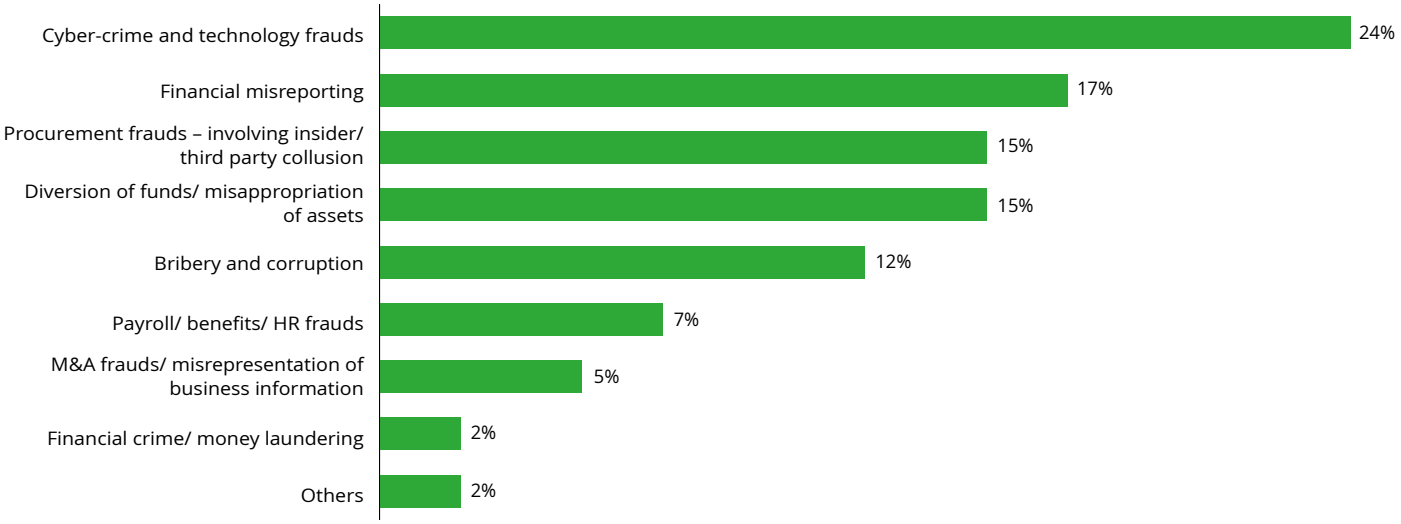
What percentage of your organisation's total revenue has been lost due to fraud in the past year?



In which areas of your business has fraud been perpetrated or is most likely to be perpetuated?



What type of fraud/misconduct/malpractice has your firm experienced over the last two years?



Note: percentages may not equal to 100 due to rounding

Due to the change in the economic environment, which of these options do you think has contributed the most to increasing your organisation's fraud risk?

23%
Technology intervention

19%
Remote working environment

17%
Performance pressure from the organisation to meet targets

15%
Financial pressure from the organisation to present favorable performance information

13%
Individual employee(s) personal finance pressure

11%
Organisation cash flow crunch

2%
Lack of process and controls

Preparedness of organisations to combat fraud risks

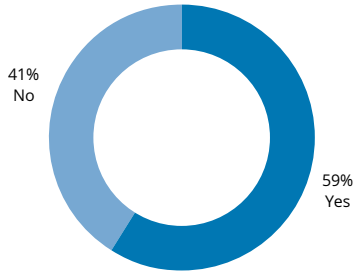
There has been an upward trend in addressing fraud in the Middle East, which indicates that companies are proactively trying to monitor various risks. However, the majority of respondents indicated that they were not confident about its effectiveness. Considering the ever-evolving and dynamic ecosystem in which organisations function, fraud prevention requires periodic or continuous risk assessments and incorporating learning from past incidents.

The increase in implementation of anti-fraud policies and related governance framework is a positive trend. However, to effectively mitigate fraud risk, companies should consider an effective anti-fraud framework comprising important elements such as an anti-fraud strategy and governance structure, policies and procedures, periodic fraud risk assessments, internal monitoring exercises involving use of tools and technologies.

41% of organisations stated that they do not have a well-established fraud risk framework to address existing and future frauds. This was corroborative from the survey where respondents indicated inefficient anti-fraud trainings and awareness of the framework in their companies. For organisations that reported having an established fraud risk framework, many also identified absence of certain necessary elements such as an effective whistle-blower mechanism, periodic senior management reporting, periodic fraud risk assessments and dedicated anti-fraud technologies.

Our survey responses indicated that proactive awareness campaigns and training for employees on emerging fraud risks resulted in reduction of fraud. However, more than 50% of respondents highlighted that there is a limited understanding of emerging fraud risks in their organisations. These organisations often place reliance on traditional techniques, static data, and irregular modification of a framework. To be better prepared, we advise organisations to shift from detective controls to implementing preventive controls by incorporating technology and using near real-time data for decision-making.

Does your organisation have an established fraud risk framework?



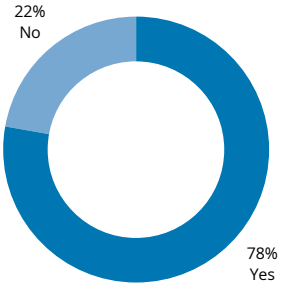
Key elements of an organisation's fraud risk framework

• Anti-fraud policy	• Anti-fraud procedure
• Code of conduct / code of ethics	• Periodic training and awareness
• Anti-bribery and corruption policy	• Periodic fraud reporting to senior management (e.g. Audit Committee of Board)
• Internal audit function	• Fraud reporting hotline / mechanism and case management tool
• Anti-fraud strategy	• Anti-fraud technology solutions – detection and monitoring
• Whistleblower policy	• Periodic fraud risk assessments

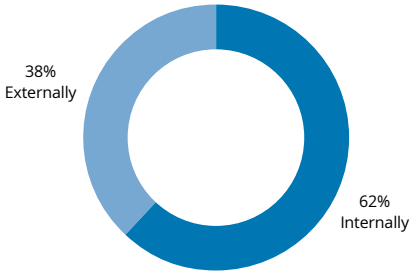
Which of the following is the most significant contributor to fraud risk in your organisation?

Note: percentages may not equal to 100 due to rounding

Does your organisation have a whistleblowing policy in place?



How is the whistleblowing facility managed?



Which of the following is the most significant challenge to the effective functioning of your organisation's whistleblowing facility?

28%
Culture of the organisation

25%
Absence of complaint follow up procedures

19%
Reluctance to whistleblowing due to fear of repercussions/ loss of job or sponsorship

16%
Protection of individuals who raise a concern

6%
Concept of anonymity

3%
My organisation's whistleblowing facility is effective

3%
Others

Corporate fraud and the role of technology

Technology is helping companies across the globe to proactively manage the risk of fraud. More than half of the respondents stated that tools and technologies used in their companies to detect fraud are effective.

We believe that investments in technology have been successful, prompting 60% of the respondents to feel that there has been a decrease in fraud cases post the implementation of fraud risk technology. The survey findings highlight that 44% of organisations place a reliance on a hybrid model (in-house and vendor dependent), for fraud risk technology services.

The findings of this survey also highlight that two-thirds of the companies have included an anti-fraud data analytics function as part of the strategic agenda. However, fraud risk technology implemented by the majority of organisations lacks predictive detection capabilities. This is an indication for companies to invest in tools such as data analytics, artificial intelligence (AI) and machine learning (ML) in order to support in detecting future frauds.

The use of AI and ML in data discovery offers numerous benefits such as locating significant documents faster, thereby increasing the efficiency and reducing costs, and also in identifying a greater volume of information to broaden and deepen the understanding of the subject matter itself.

The survey indicates that most of the organisations are currently using technology to mitigate fraud risks. This advancement makes it possible for companies to build and optimise enterprise-wide visibility for addressing fraud risk concerns. Organisations should consider investing in technologies that can be customised and scalable as per their needs with the help of subject matter experts. Unless such technology investments are made, companies may find it difficult to combat the rapidly evolving frauds in the present digital age.

How effective are the tools and technologies used in your organisation for detecting fraud?

Very effective
24%

Effective
28%

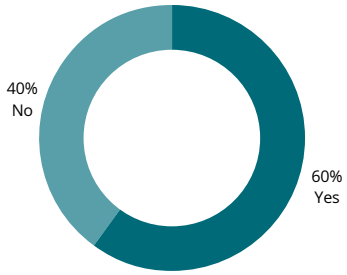
Unknown
3%

Ineffective
10%

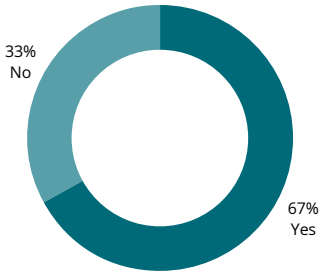
Neither
14%

We do not use tools and technologies for detecting fraud
21%

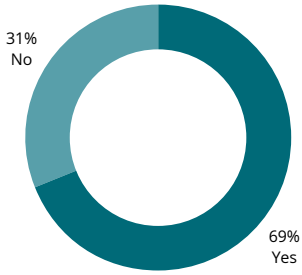
Have you seen a decrease in fraud cases post the implementation of the fraud risk technology?



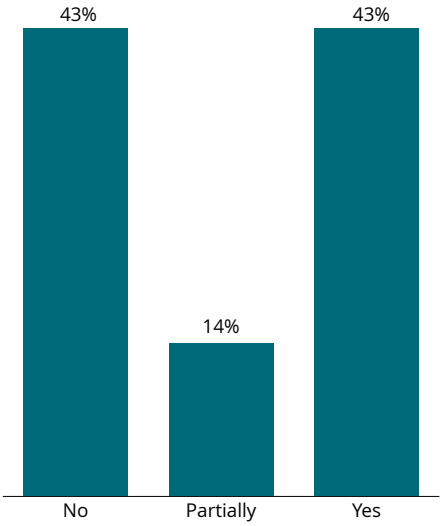
Does your fraud risk technology have any predictive detection capabilities such as artificial intelligence and machine learning?



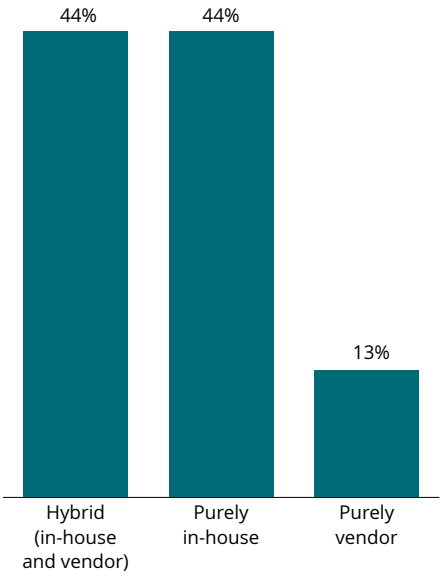
Does your organisation have the anti-fraud data analytics function on the strategic agenda of the CIO/CTO/CDO?



Is the fraud risk technology used in your company fully operational?



What type of fraud risk technology is used in your organisation?



Note: percentages ma not equal to 100 due to rounding

The last word

A decade ago, fraud prevention and detection was not a common subject compared with today, as greater reliance was placed on compliance and internal audit professionals to identify fraud within an organisation. Over the years, while the reliance on internal auditors has remained, there is an equal emphasis on bringing forensic professionals onboard with specialised skill sets to advise and support on prevention, detection and response.

As mentioned in the report, 41% of the companies did not have an established fraud risk framework. This could be indicative of the reliance that many organisations still place on traditional methods of fraud detection such as the analysis of static data, internal audit and irregular reviews of their fraud risk. However, the pandemic has revealed that this may not be sufficient for most organisations. We recommend adopting a proactive approach to combat fraud risks.

The past few years have seen an increased number of regulatory actions globally against individuals and companies due to instances of fraud. There is a need for organisations to effectively manage their fraud framework to ensure the availability of source information to aid investigations should there be any reported instances of frauds. This underscores the importance of being able to readily access and extract data from the company's prevention detection tools in order to investigate and respond to requests from regulators in case of regulatory actions.

In our view, an enterprise-wide fraud risk framework is essential for fraud prevention. The maturity level of technology in the market makes it possible for companies to build and optimise enterprise-wide visibility for fraud. Successful and effective fraud risk management functions are those that continuously review and refine their working relationships and processes with specific internal and external stakeholder groups, and act and operate as an integrated seamless function of the organisation. This ensures constant assessing of the performance against industry practices and benchmarks while actively combatting fraud.

We believe that the future of fraud risk management will be a collaborative effort within this ecosystem of experts. While we are concerned about the lack of fraud management preparedness across organisations, we have witnessed instances where internal and external collaborations have driven and enhanced the effectiveness of organisations' fraud risk management efforts.

Key contacts

Neil Hargreaves
Partner
Head of Forensic
Deloitte Middle East
+971 50 650 6214
nehargreaves@deloitte.com

Collin Keeney
Partner
Forensic
Deloitte Middle East
+971 50 650 1829
ckeeney@deloitte.com

Prabodh Newar
Assistant Director
Forensic
Deloitte Middle East
+971 55 802 1365
pranewar@deloitte.com

Deloitte.

Designed by Deloitte CoRe Creative Services. RITM0817720