IMPLICATION OF PANDEMIC ON FRAUD RISK

FRAUD INSTANCES HAS INCREASED DURING PANDEMIC ACROSS INDUSTRIES

RSM INDONESIA SPECIAL REPORT

THE POWER OF BEING UNDERSTOOD

AUDIT | TAX | CONSULTING

RSM

BE MINDFUL TO THREATS AROUND YOUR ORGANIZATION

As Covid-19 continues to reach new milestones and further impact the economy, businesses are experiencing unprecedented disruption. From supply chain issues and diminished workforce mobility, to severe supply chain interruption, threats to organizations are real and intensifying rapidly. Even more, we are facing the new era that requires the usage of technology to conduct regular activities such as meeting with clients or colleagues, virtual payment, online shopping, etc. Everyone should be aware of new potential fraud occurred by using technology, better known as cybercrime.

We conducted an online survey about threats to organizations with respondents from 18 industries with the majority (70%) of job responsibilities have ties to risk management practices.

This survey was intended to get a better understanding of fraud or potential fraud that may occur, considering the increase of technology usage during this pandemic. We believe this survey will increase our awareness of potential fraud as it can happen around your organization.

SNAPSHOT OF THE SURVEY

DEMOGRAPHIC

130+ Respondents **from** 18 industry sectors

80% of respondents stated that fraud in their organizations has increased during the pandemic

ASSET MISAPPROPRIATION

35% is the most common fraud occurred in respondents' organization during pandemic

46% Almost half of the respondents stated that their middle level management were the ones who committed fraud

70% of the fraud perpetrators likely age range **30 – 39 years old**

Most Proven Initial Way of Detecting Fraud

53% Internal Audit

29% Whistleblowing Channel

32% respondents **EMAIL** is the formal reporting mechanism most often used by whistleblowers

20% respondents stated that their organization **still does not** have any formal channel to report violations

52% of respondents cited fear of bad publicity as the main reason on why some organizations decline to refer their financial crime cases to the law enforcement

Two impacts of fraud that organizations fear the most

36% Financial loss

35% Collapse of reputation

56% of respondents believe that their organization's revenue would be affected the most by the Covid-19 pandemic

RESPONDENTS

This survey focuses on the 132 respondents from individuals that are mostly responsible for aspects of GRC internal to their organization's operations. The survey was fielded at the mid of 2020.

The largest array of the respondents came from Government (21%), followed by Banks (15%) and Commercial & Professional services (9%) – all from Indonesia.

DEMOGRAPHIC

INDUSTRY

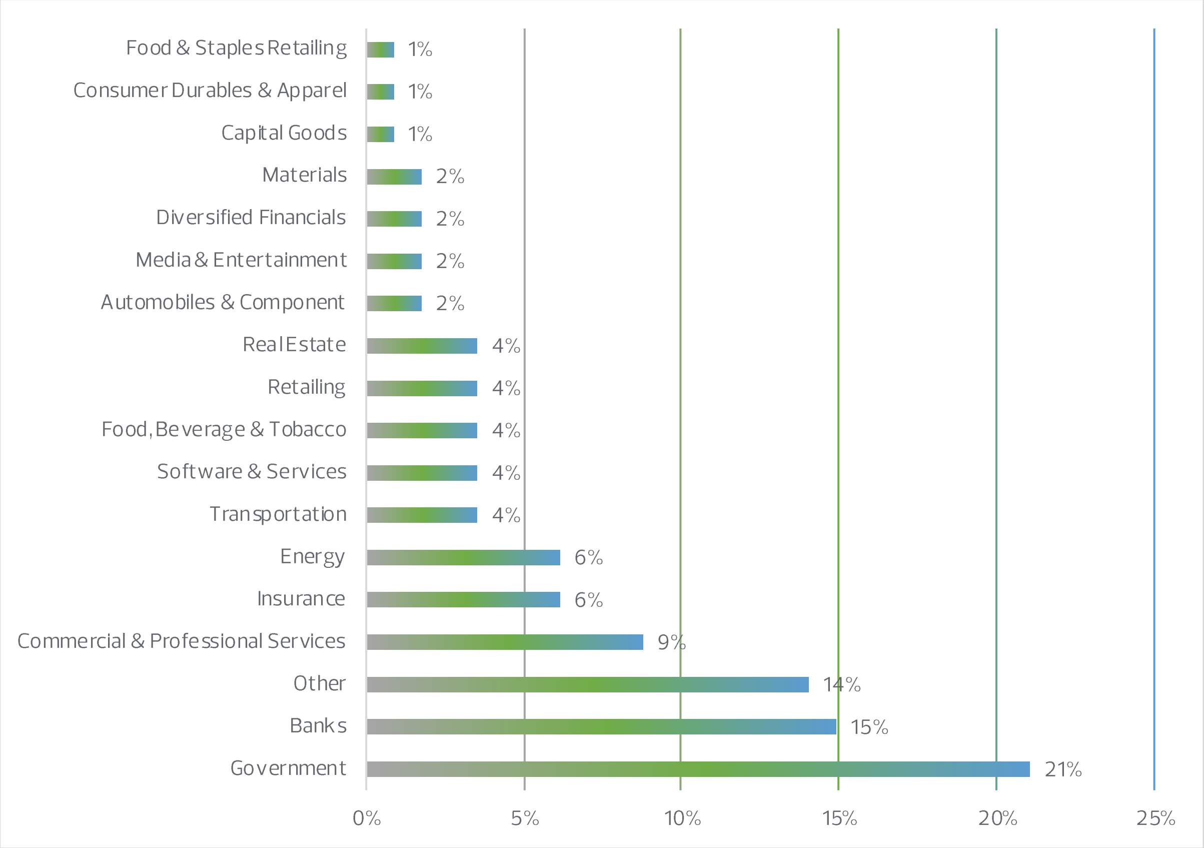

Figure 1: Industry

SIZE OF ORGANIZATION

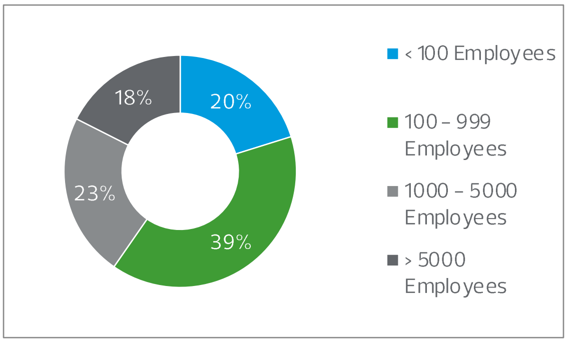

Figure 2: Number of Employees

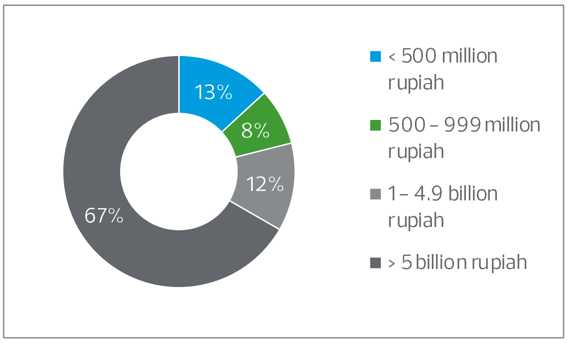

Figure 3: Annual Revenue

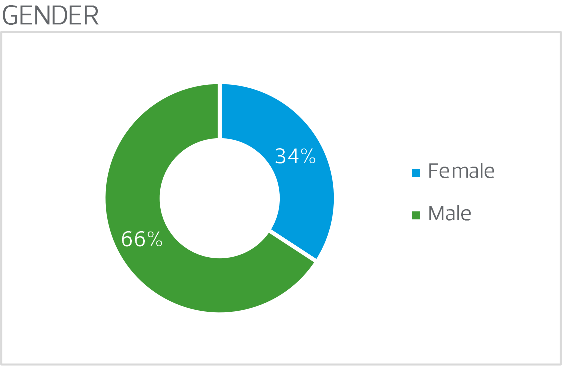

Figure 4: Gender

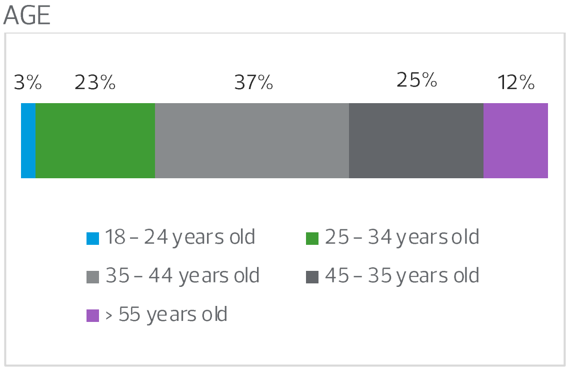

Figure 5: Age

TYPES OF MISCONDUCT

Fraud is any intentional act or omission designed to deceive others, resulting in the victim suffering a loss and/or the perpetrator achieving a gain[1]. Referring to Fraud Tree (Occupational Fraud and Abuse Classification System) there are 3 major types of occupational fraud: Corruption, Asset Misappropriation, and Fraudulent Statements.[2]

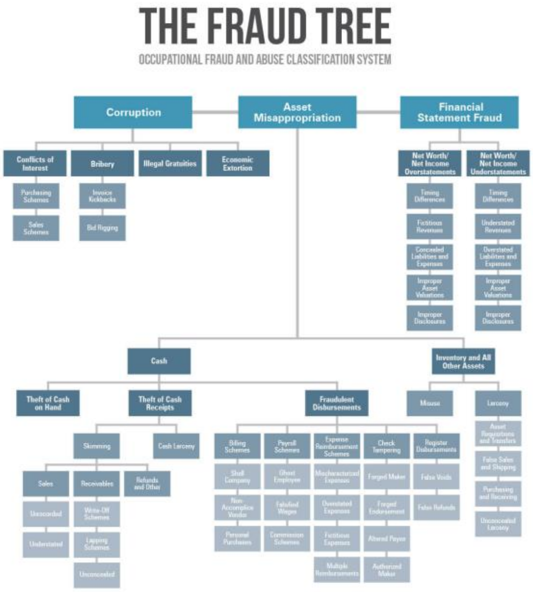

Figure 6: Fraud Tree

Nowadays, data and interconnectivity are crucial elements for the industries. Smart manufacturing offers some new benefits, such as greater access to data across the entire supply chain network, higher quality products and innovation, more manufacturing jobs and energy efficiency. On the other hand, the characteristic of their interconnectivity carries some risks to their data security. It creates a big opportunity for those who wants to do cybercrime such as hacking, malware, social engineering, privilege misuse, etc. since they understand that the security system will be vulnerable to be exploited due to the fact that there are other connecting devices. Therefore, in this survey we also add cybercrime to the category due to the increase of technology usage.

[1] Committee of Sponsoring Organizations of the Treadway Commission (COSO) – Fraud Risk Management Guide Executive Summary, p. 3

[2] Association of Certified Fraud Examiners (ACFE)

SUDDEN SHIFT TO VIRTUAL WORKING ARRANGEMENT HAS INCREASED CYBERSECURITY THREATS AS WELL AS FRAUD INSTANCES TO MANY ORGANIZATIONS, ESPECIALLY THOSE THAT HAVE WEAKNESSES IN THEIR INTERNAL CONTROL SYSTEM.

CURRENT CHALLENGES

In this time of pandemic, changes in how people do their work are inevitable. Almost all respondent (93%) stated that their organization implement WFH. Only 6% did not, and 1% working with shifts.

Many organizations decided to implement work from home (WFH) system and advise their employee to stay safe at home and not conducting activities as the way it used to be and using video conferencing applications to communicate with each other and other virtual working arrangement in replacement of the previous physical attendance. The Ministry of Communication and Information Technology also stated that the use of internet applications has been increased up to 40% during the pandemic.[3]

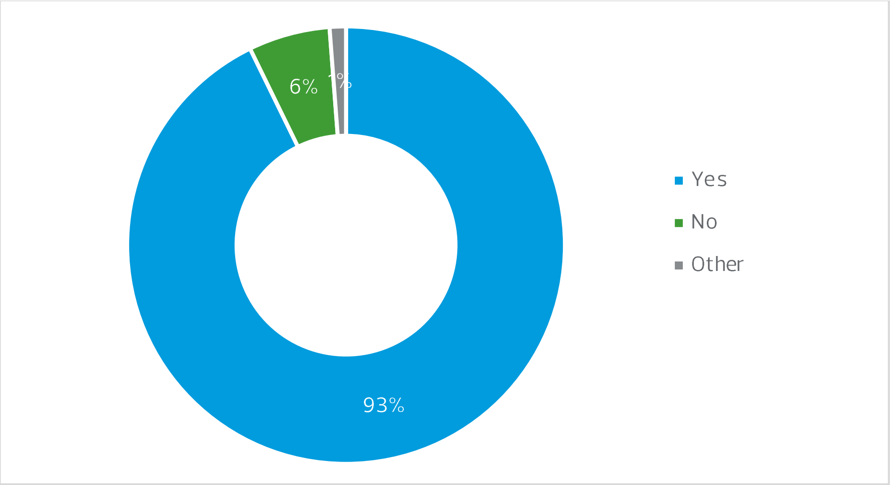

Figure 7: During this pandemic, many companies implemented Work from Home, is your company one of them?

With the increase of virtual mode in working, there is an increase on the potential for cybersecurity threats due to the use of virtual private networks (VPN), mobile devices, or third-party applications to support activities of employees who work remotely and/or WFH that is not accompanied by adequate security systems.

[3] Ministry of Communication and Information Technology of Republic Indonesia

INFORMATION AND DATA SECURITY CONCERNS DURING PANDEMIC

Nowadays, online meetings and other virtual interactions become very commonly used and unfortunately, can pose new risk of fraud if the security of organization's information and data are not well preserved.

Almost half of the respondents (41%) believe that the security of their organization information and data are well preserved along with the increasing of virtual interaction at work, while 32% respondents are not too confident about that.

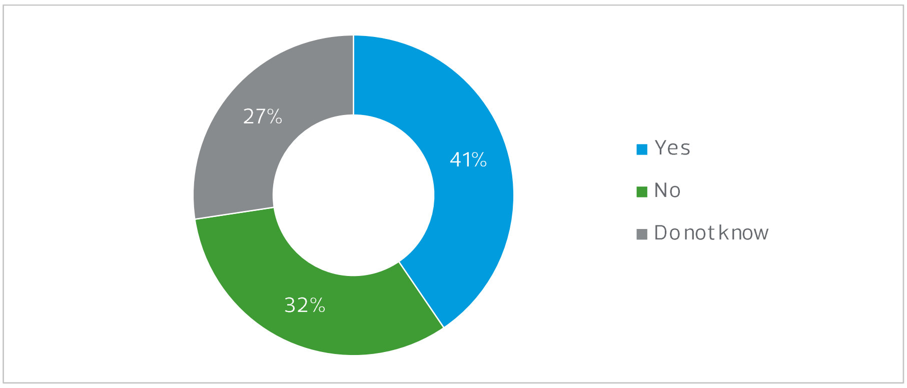

Figure 8: With the increasing of virtual interaction at work, are you sure that the security of your company's information and data is well preserved?

INCREASE OF FRAUD INSTANCES DURING PANDEMIC

Majority of the respondents (80%) stated that fraud in their organizations increased during this pandemic. 8% respondents stated there was no increase in fraud, while the other 12% respondents did not know because there is no specific assessment for it yet.

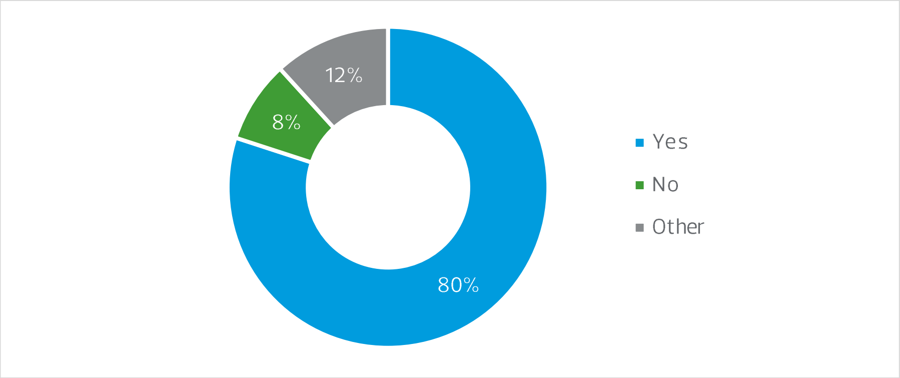

Figure 9: Does fraud instances increase during this pandemic?

Companies have increasingly become the target for cybercriminals, with data incidents rising incrementally each year. Attackers typically know that large organizations have invested heavily in security. In addition, the Covid-19 pandemic has increased the complexity of cybersecurity challenges for the middle market. As the organization has become even more dependent on the internet to remain productive, hackers are taking advantage of the crisis by unleashing a variety of attacks. In an unprecedented public health situation, where organizations must focus on employee safety and keeping the business running, cybersecurity processes require heightened attention.[4]

[4] RSM US Middle Market Business Index – Cybersecurity: https://rsmus.com/economics/rsm-middle-market-business-index-mmbi/cybersecurity-special-report.html

MANY PERCEIVED THAT MID-MANAGEMENT LEVEL AND IN THE AGE RANGE OF 30-39 YEARS ARE MOST POTENTIAL FRAUDSTER, THIS MIGHT BE DUE TO THE PERCEPTION THAT MANAGEMENT LEVEL HAVE MORE ACCESS AND OPPORTUNITY.

POTENTIAL FOR FRAUD

Fraud can be conducted by everyone, either from the inside or the outside. Internally, fraud can be committed by the operating level management to the top-level management. While externally, fraud can be committed by customers, vendors, or other parties.

WHO ARE PERCEIVED AS HIGH RISK FOR COMMITTING FRAUD

When asked about who has the highest potential to commit fraud in the organization, most respondents (68%) believed that management levels have the highest potential. The second is non-management level/staff (26%). In several other organizations, consumers/customers and owners have the highest potential for committing fraud.

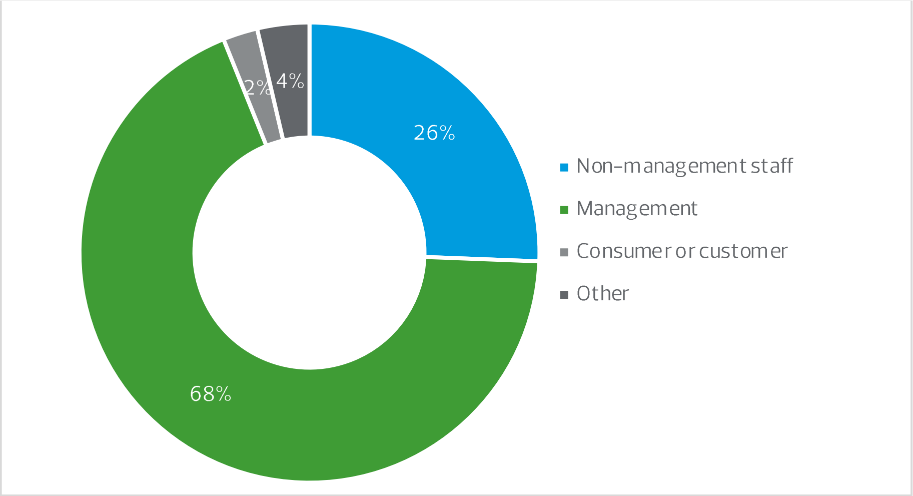

Figure 10: I n your opinion, who has the highest potential for misconduct in an organization?

AREA THAT POSES THE GREATEST RISK FOR FRAUD

Almost half of the respondents believe that Procurement is the function that would be posing the greatest risk for fraud (49%).

During the pandemic, procurement fraud is very likely to occur in organizations. Corruption can occur at every stage of procurement, from planning, selecting providers, to payments and audits, there are also possibility of a price mark-up in the procurement process. The process of procuring goods/services must be carried out carefully because the current emergency has caused prices to soar up.

For other function, Finance and Accounting is chosen as the runner up by 25% of the respondents while on the third to fifth position in order are Sales Department (15%), Human Resources Department (7%) and Information Technology Department (4%).

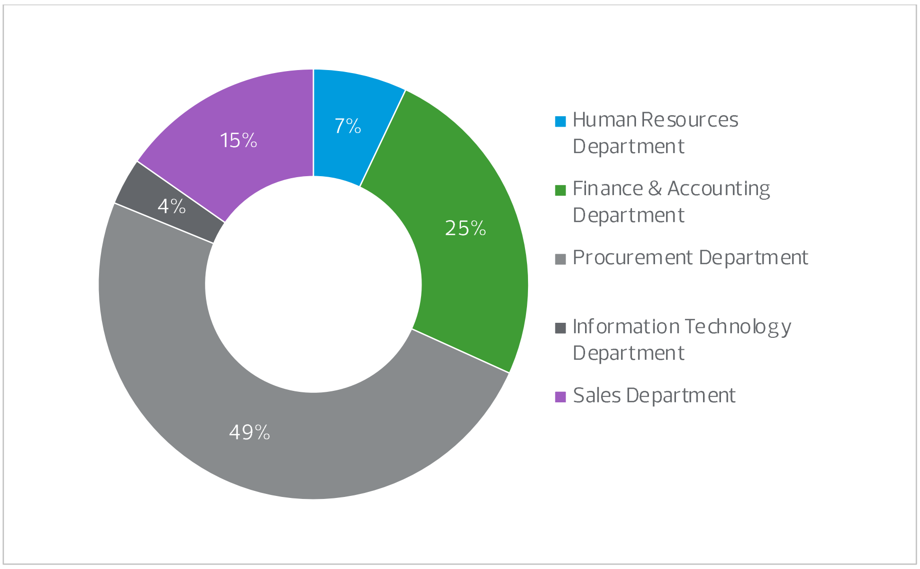

Figure 11: What departments pose the greatest risk for fraud?

Top-level management and personnel at all levels of the organization have responsibility in managing fraud risk. They are expected to understand how the organization is responding to fraud; what form of Fraud Risk Management Program the organization has in place; how it identifies fraud risks; what it is doing to better prevent and detect fraud; and what process is in place to investigate fraud and take corrective action.

There are WAYS TO IMPLEMENT AN EFFECTIVE FRAUD CONTROL within an organization, which include:

1. MANAGEMENT. Fraud can happen even in an organization that has strong ethical culture. Management includes anti-fraud personnel in the preparation process of designing policy and procedure to bring fraud risks awareness to the organization.
2. INTERNAL AUDITOR. Conduct the engagement plan review and make an adjustment, as the organization needed to prioritize assignment to fraud risk. Explore related resources to help internal auditor understand more about their challenging role caused by Covid-19 pandemic.
3. EXTERNAL AUDITOR. Review of current risk assessment results are needed, as a consideration of the pandemic impact on financial statements area.
4. DIRECTORS AND AUDIT & RISK COMMITTEE. Re-assessment of risk profile in the organization, identifying the impact of work-from-home to the internal control environment, updating control design, build awareness on fraud risks and keep the scepticism as one of the anti-fraud key components.

ASSET MISAPPROPRIATION HAS HAPPENED DURING THE PANDEMIC IN FORM OF THEFT OF CASH, FRAUDULENT DISBURSEMENT. DETECTION WAS MOSTLY DONE THROUGH INTERNAL AUDIT AND FROM TIPS SUBMITTED THROUGH THE WHISTLEBLOWING CHANNEL.

FRAUD OCCURENCE DURING PANDEMIC

TYPE OF FRAUD OCCURED MOST FREQUENTLY

In 2020, Covid-19 had causes unprecedented job crisis, almost all workers and businesses are affected. Large-scale social restrictions (PSBB) for health and safety reasons imposed in various regions in Indonesia forced businesses to adapt quickly in order to survive. However, not all organizations are prepared for such rapid adaptation and change, which can create new fraud risks in their business.

Most respondents (35%) stated that asset misappropriation has occurred in their organization in the past months after the corona hit. It can be seen in the form of theft of cash on hand, theft of cash receipts, fraudulent disbursements, misuse inventory & all other assets, and larceny inventory & all other assets. Other respondents (18%) stated that corruption occurred in their organization, followed by cybercrime (4%) and financial statement fraud (3%).

Meanwhile, some respondents (25%) stated that there was no fraud in their organization during this period, and the rest of respondents did not know whether there was fraud that occurred in their organization or not (15%).

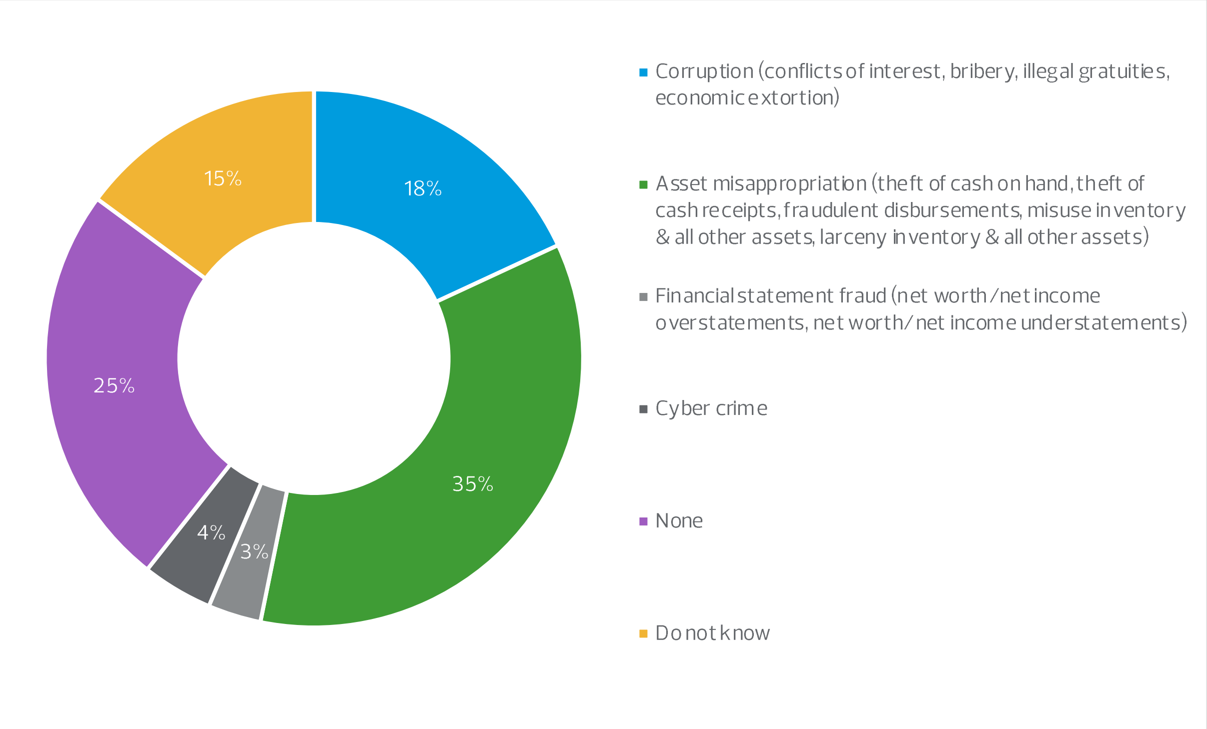

Figure 14: What fraud have your organization experienced in the past 6 months?

WAYS TO DETECT FRAUD

It seems impossible to eliminate all fraud in all organizations. However, implementation of an effective fraud control will minimize the fraud risk and create a strong fraud deterrence effect. Internal audit has proven to be the initial way of detecting fraud in most respondents' (53%) organizations, followed by tips or whistleblowing channel (29%).

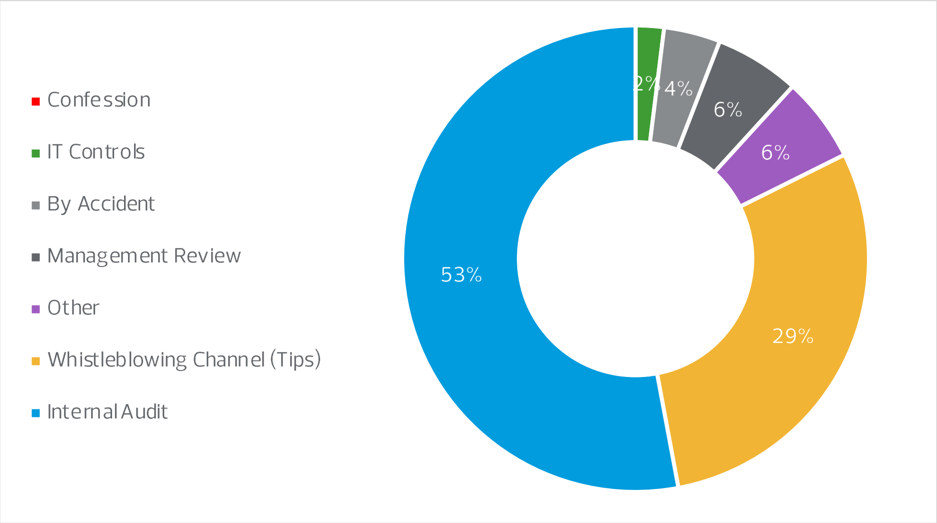

Figure 15: How was the fraud initially detected?

FORMAL VIOLATION REPORTING MECHANISMS USED

We also asked the respondents about the formal reporting mechanism used in their organization to receive reports about violation to laws, regulation, and breach of ethical conduct. Most respondents (32%) use email as their formal reporting mechanism. In several other organizations, the reporting mechanism use text message (18%), mail (16%), or web based (14%). Meanwhile, 20% of respondents stated that their organization does not have a formal reporting mechanism or whistleblowing system.

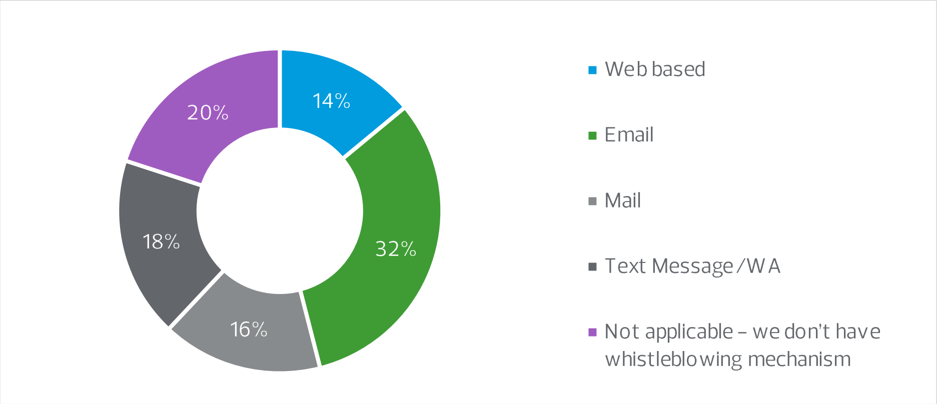

Figure 16: What formal reporting mechanisms did whistleblowers use?

Our survey shows that there are organizations that still have not used the whistleblowing system, while it is an important source to help the top level management to minimize a wide range of risks, discover fraud and even prevent the potential fraudster to commit the fraud. Whistleblowing gives every personnel in the organization the opportunity to report a concern if they see something is suspicious against the organization's ethical principles. The ACFE's Report to the Nations showed that organizations that did not have a whistleblowing system in place suffered losses that were twice the size compared to those who did have a whistleblowing system.

PERPETRATOR OF FRAUD BY WORK LEVEL

Our survey finds that in their organization, almost half of the respondents (46%) stated that their middle level management was the one who committed the fraud, followed by top level management (27%) and operating level management, while 12% answered other. For those who answered other, they stated that fraud was committed by external parties such as customers or vendors.

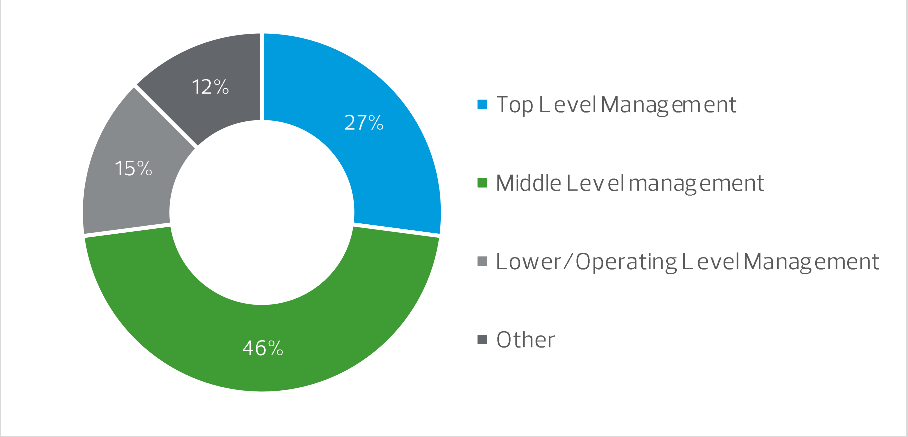

Figure 17: Who committed the fraud?

PERPETRATOR OF FRAUD BY AGE GROUP

Fraud can be committed by people of all ages. In this survey, we divide the fraudsters into four (4) age groups from 20 years old to more than 59 years old.

Majority of respondents (70%) stated that people who committed fraud is likely to be in 30–39 years old, followed by 20–29 years old (19%).

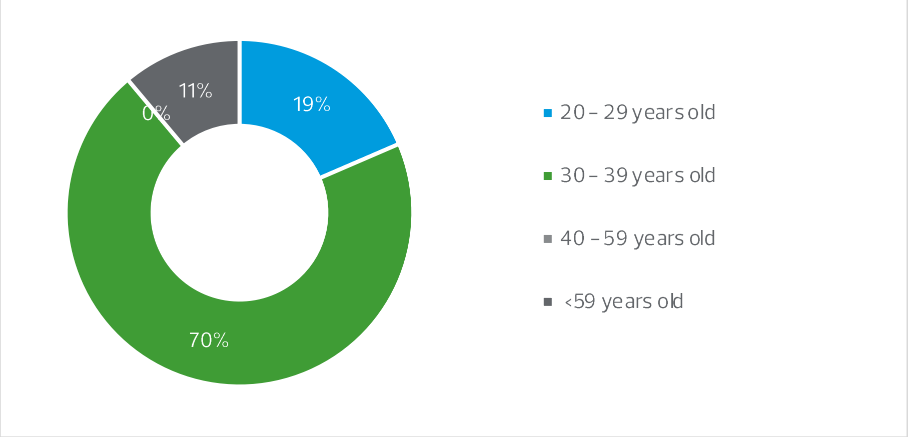

Figure 18: How old is the person who committed the fraud?

FEAR OF BAD PUBLICITY WAS ON THE TOP OF MIND WHEN FRAUD HIT, AND FOR THE SAME REASON, SOME OPT OUT FROM REPORTING IT TO LAW ENFORCEMENT. UNFORTUNATELY, THIS PREVENT ORGANIZATION TO SHOWCASE A LESSON LEARNED TO OTHERS.

FRAUD IMPACT

THE IMPACT OF FINANCIAL CRIME

Most respondents sees financial loss (36%) and the collapse of the company's reputation (35%) as the worst impact of financial crime that their organizations avoids, while 25% respondents believe that disruption of their operational activities would be the worst impact of financial crime.

Among the respondents that chose the "other" option, about two respondents explained that all of the options especially financial loss and affected company's reputation are equally worst and one other respondent believe that data security and integrity would be the worst impact of financial crime.

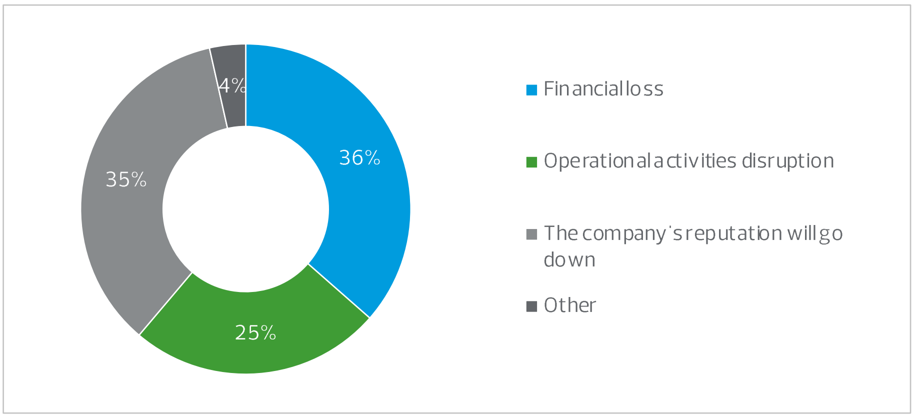

Figure 12: What is the worst impact of financial crime that your organization avoids?

WHERE PANDEMIC HIT THE MOST

More than half of the respondents believe that their company's revenue would be affected the most by the Covid-19 pandemic (56%). Almost every company are affected by the pandemic. Some of the hardest hit industries such as travel, tourism, and hospitality industry has affected greatly for the past 6 months due to large-scale social restrictions and decreased demand. But in some industries, it is the other way around. For example, revenue in the logistics industry has increased due to shifting patterns of consumer spending from offline to online.

31% respondents believe that the human resources would be affected the most. In this pandemic era, where companies must be able to adapt quickly so that business can continue to run effectively and efficiently, Human Resources Department faced extraordinary challenges in managing its employees and to maintain their productivity without compromising their health and safety.

Other 7% answered information technology, 4% answered financial crime, and 2% respondents explained that the production or missed performance targets would be the most affected areas.

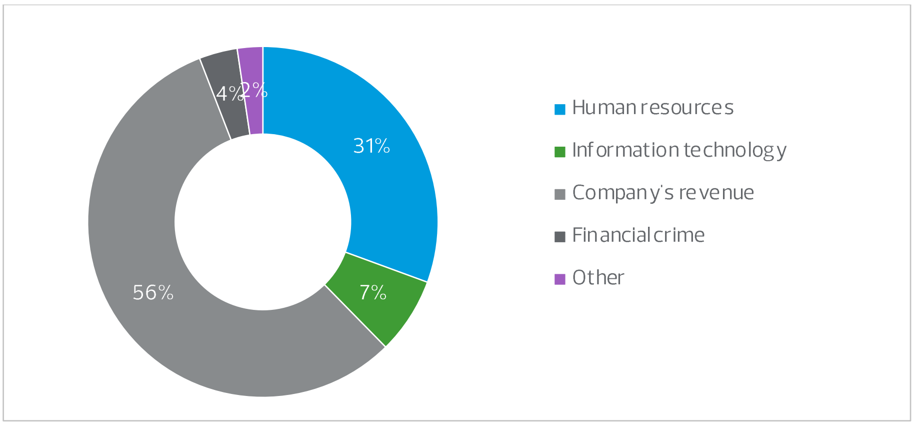

Figure 13: With the Covid-19 pandemic, which areas in your company are most affected?

RELUCTANCY IN TAKING FRAUD CASES TO LAW ENFORCEMENT

More than half of the respondents (52%) believe that fear of bad publicity is the main reason on why the organizations decline to refer cases to the law enforcement.

26% of the respondents thought that the process will be very costly. 12% respondents are confident that its unnecessary for organizations to refer fraud cases happened on them to the law enforcement because their internal discipline is already sufficient.

On the other hand, 8% of the respondents explained that solving problems in a friendly manner, complicated bureaucracy, uncertainty of results, as well as a combination of all the reasons mentioned are among the reasons on why organizations decline to refer cases to law enforcement. Remaining 2% of the respondents explained that because the perpetrator already disappeared, there is no urgency to work with the law enforcement to solve the case.

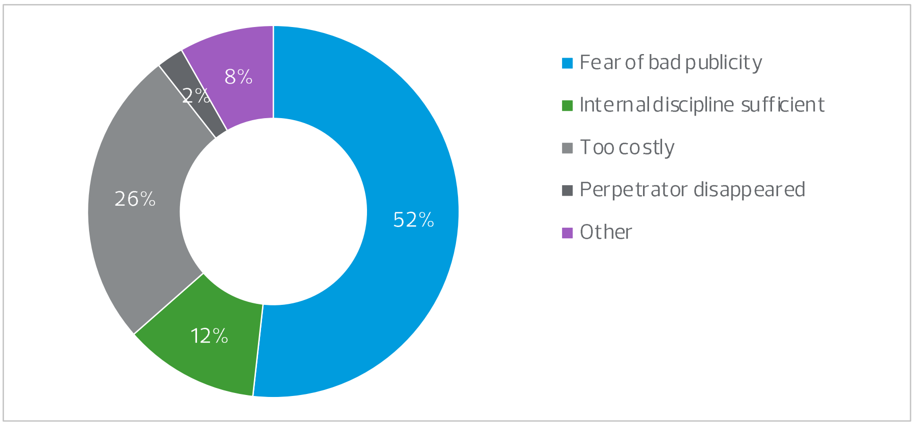

Figure 18: Why do organizations decline to refer cases to law enforcement?

The widespread of fraud is caused by lack of fraud prevention in the company itself. With the number of fraud cases that are gradually increasing, organizations are encouraged to conduct an integrated approach in the implementation of corporate governance.

It is important to ensure that these principles do exist and functioning in managing fraud risk:

1. CONTROL ENVIRONMENT. Integrity and ethical value are fundamentals in managing and preventing fraud. It addresses culture and way the people within the organization meet their respective obligations to achieve the organization's goals, including fiduciary, reporting, and legal responsibilities to stakeholders.
2. FRAUD RISK ASSESSMENT. Identify fraud scheme and fraud risk. Addressing the actual risks that are faced by organization as determined by its purpose. The goal is to determine the type, likelihood, and potential cost of risks in a traditional expected value framework. It allows organization to tailor program efforts toward cost effective mitigation.
3. DESIGN AND IMPLEMENT ANTI-FRAUD CONTROL ACTIVITIES. Design a preventive and detective anti-fraud control activities, such as policies and procedures, to mitigate fraud risks or the inability to detect fraud in time.
4. SHARING INFORMATION AND COMMUNICATION. Acquire information to potential fraud.
5. MONITORING ACTIVITIES. Organization need to evaluate sustainably to ensure the principle of fraud risks are operating. One of fraud prevention key element is to set up responsibilities and processes to ensure that the information is reported to someone who can address the problem.

MOST ORGANIZATIONS BELIEVED THAT THEY HAVE PUT MEASURES AND SAFEGUARD TO PREVENT AND DETECT FRAUD, AND THIS HELPS IN MANAGING FRAUD RISKS WITHIN.

FRAUD PREVENTION AND DETECTION

PREVENTION AND DETECTION PROCEDURES IN ANTICIPATION OF FRAUD

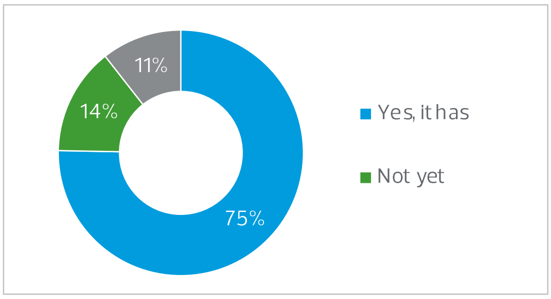

Figure 19: Has your company carried out prevention and detection procedures in anticipation of fraud against your company?

75% of the respondents answered that their company had carried out prevention and detection procedures in anticipation of fraud against their company, while 14% respondents answered not yet, and 11% respondents said they did not know if their company has carried such procedures.

SAFEGUARD TO FRAUD

Majority of the respondents (27%) believe that conducting internal audit regularly would be the best precaution for fraud, while 23% of respondents believe that implementation of whistleblowing system would be the best way.

Other than that, increasing IT Security (18%), employee rotation (17%), and pay attention to employee's financial wellbeing (15%) voted by approximately the same number of respondents as the best precaution of fraud.

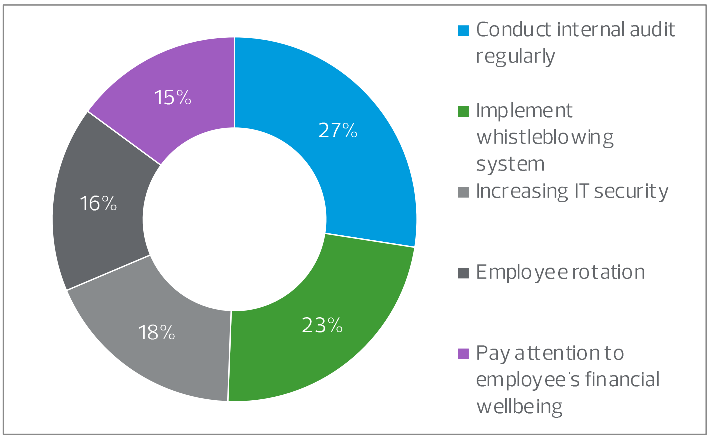

Figure 20: What is the best precaution of fraud?

INFORMATION TECHNOLOGY TO REDUCE THE POSSIBILITY OF FRAUD

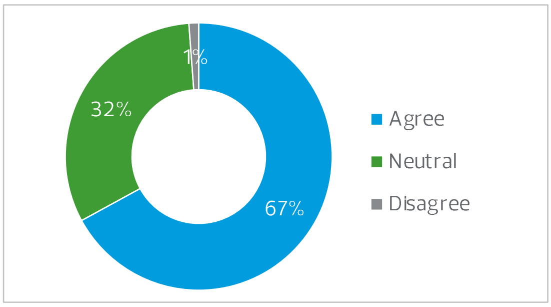

Figure 21: Does intensifying the use of IT in your organization can reduce the possibility of fraud?

Majority of the respondents (67%) agree that the possibility of fraud in their organization can be reduced by intensifying the use of IT. Meanwhile, 32% of the respondents remained neutral and only 1% respondent disagree with the notion.

GOVERNING AND MANAGING PERFORMANCE, RISK, AND COMPLIANCE ARE KEY IN ANY ORGANIZATION, REGARDLESS OF SIZE AND INDUSTRIES. ENHANCEMENT IN THE GOVERNANCE, PROCESSES AND CONTROLS AS WELL AS BUILDING A STRONG ETHICAL CULTURE ARE NEEDED.

KEY TAKEAWAY

Governance | Risk | Ethics & Compliance | Finance | Technology | Audit | Legal | Core Process

GOVERNANCE

REVISIT GOVERNANCE MODEL

Good governance is the bedrock of all successful organizations. If this goes wrong the ramifications can be deeply damaging. Where organizations get it right, they can become more efficient and effective.

It is quite straightforward really, the less that goes wrong in your organization, the less (unexpected) cost you will incur when putting it right.

The reality is that few organizations take stock and ensure their governance arrangements are as effective as they should or could be. This often only changes when the organization is driven by regulators to do so, or when the cracks are starting to show – though by then it is often too late.

There should be effort to review and refine the governance model and practices.

STRENGTHEN THE THREE LINES MODEL

To ensure sound implementation of the governance model, organizations need to strengthen the effectiveness and cohesiveness of the three lines within the organization.

- Adopting a principles-based approach and adapting the model to suit organizational objectives and circumstances.
- Mapping the existing functions and its roles and re-aligning it for betterment.
- Reducing or eliminating unnecessary reporting lines.
- Enhancing the quality of reporting so that it will be more valuable to the governing body.
- Never stop reminding everyone within the organization that risk management is management's responsibility and predominantly the first line is responsible to manage risk in their day-to-day operations.
- Encouraging and promoting the needs and practice of effective communication between key roles.

More of collaboration and communication as well as less of silos and duplication, supported with clear roles and its segregation will be positive for any organization, regardless of size and sectors.

PROCESSES AND CONTROLS

STRENGTHEN INTERNAL CONTROL

Once fraud occurs, people then would realize that there are some weaknesses in their fraud controls. An organization need to enhance their controlling activity, since fraud happened quite frequent recently.

Internal control framework provides a road map regarding the control environment, how people relate to each other and communicate, organization structures and governance process. It is designed to safeguard organization's assets, ensure the integrity of its records, also prevent and detect irregularities or fraud. Internal control should be monitored and revised on a consistent basis to ensure they are effective and current with technological and other advances.

EMPOWER INTERNAL AUDIT

Internal audit can play an important role in helping top management weigh in the opportunities and risks in the decision-making process. Internal audit should be able to contribute in practical ways and help solve crises effectively, starting from overcoming current problems faced, overcoming short-term possible risks, to providing long-term risk management while learning valuable lessons from this pandemic. At the same time, internal audit must be able to provide guarantees and insights about the risk and risk responses of "business as usual".

FRAUD PREVENTION

BUILD ETHICAL CULTURE

Organizations must not just talk the talk; they must walk the walk by establishing an ethical environment for conducting business. Create a culture that expects employees to conduct themselves in an ethical manner, and foster an environment where employees are comfortable being uncomfortable.

In an ethical culture, pressure to commit fraud is counteracted through sound risk management strategies and appropriate incentives. It will support well-designed controls that reduce opportunities for fraud and increase the likelihood of early detection. A culture of honesty limits an individual's ability to rationalize fraudulent actions.

HAVE A WHISTLEBLOWING SYSTEM

Every organization should offer its stakeholder the opportunity to report wrongdoing comfortably via a trusted and easily accessible whistleblowing channel, to make the process of raising concerns as simple as possible.

An effectively implemented whistleblowing program can provide early warning of wrongdoing and alleviate the risks that your organization face today. Having a whistleblowing program in place is also part of an anti-bribery management system and demonstrates the leader's commitment to ethical culture.

STRENGTHEN FRAUD RISK MANAGEMENT

Today's organizations are more complex than ever before. Thanks to advances in information technology, risks travel and multiply faster than ever. In addition, the business landscape is more complex with disruptive technologies and competition. As a result, organizations have less time to respond to threats and seize emerging opportunities, and must become more proactive in identifying, assessing, and managing risk.

The field of risk management has attracted increased mainstream attention in the wake of the economic meltdown as the public has begun to comprehend the negative effects of uncontained risk. As organizations increase their focus on risk, they should take the opportunity to consider, enact and improve measures to detect, deter and prevent fraud.

For more information on RSM, please visit **www.rsm.id**

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal, or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM in Indonesia, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM is represented in Indonesia by the following member firms: KAP Amir Abadi Jusuf, Aryanto, Mawar & Rekan, PT RSM Indonesia Konsultan, PT RSM Indonesia Mitradaya, PT RSM Indonesia Mitradana. RSM's Indonesian member firms work closely together within Indonesia. Each firm is a separate and independent legal entity and a member of the RSM International, a global network of independent audit, tax, and consulting firms. Each member firm is responsible only for its own acts and omissions, and not those of any other party.

RSM