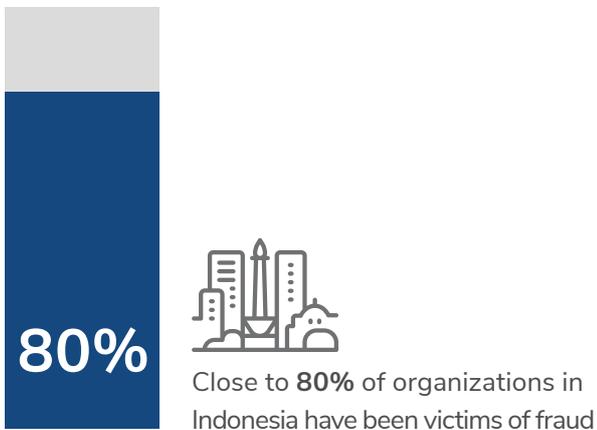


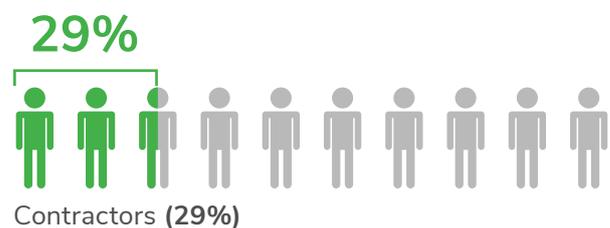
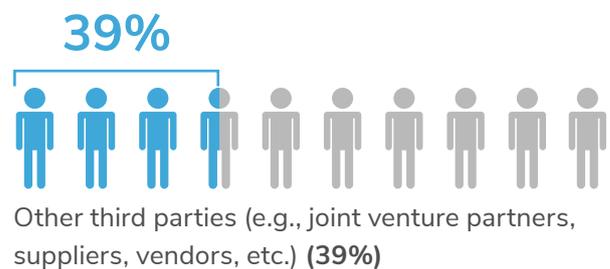
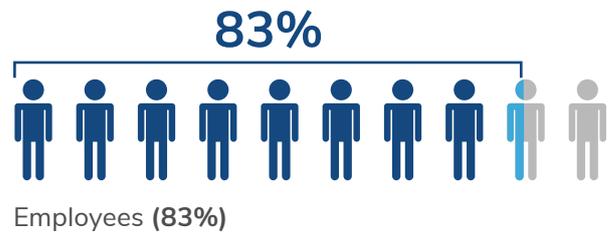


Kroll/ACFE Indonesia Fraud Risk Survey

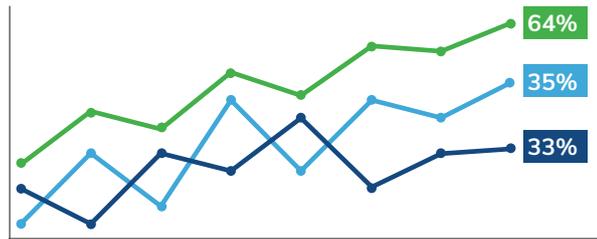
Key findings:



Key perpetrators of fraud incidents were:



Top three incidents that have significantly affected organizations in the last year:



-  Fraud by internal parties (64%)
-  Bribery and corruption (35%)
-  Fraud by external parties (33%)

Whistleblower program



Internal audit



Majority of incidents were detected via a whistleblower program (62%) or internal audit (52%)



Loss of USD 69,000/ IDR 1 billion a year

Cost of fraud: 32% of the organizations suffered a loss of more than USD 69,000/IDR 1 billion a year due to the incident(s)

86%



86% of organizations investigated these incidents internally and 34% attempted to recover the losses whereas only 15% disclosed the incident

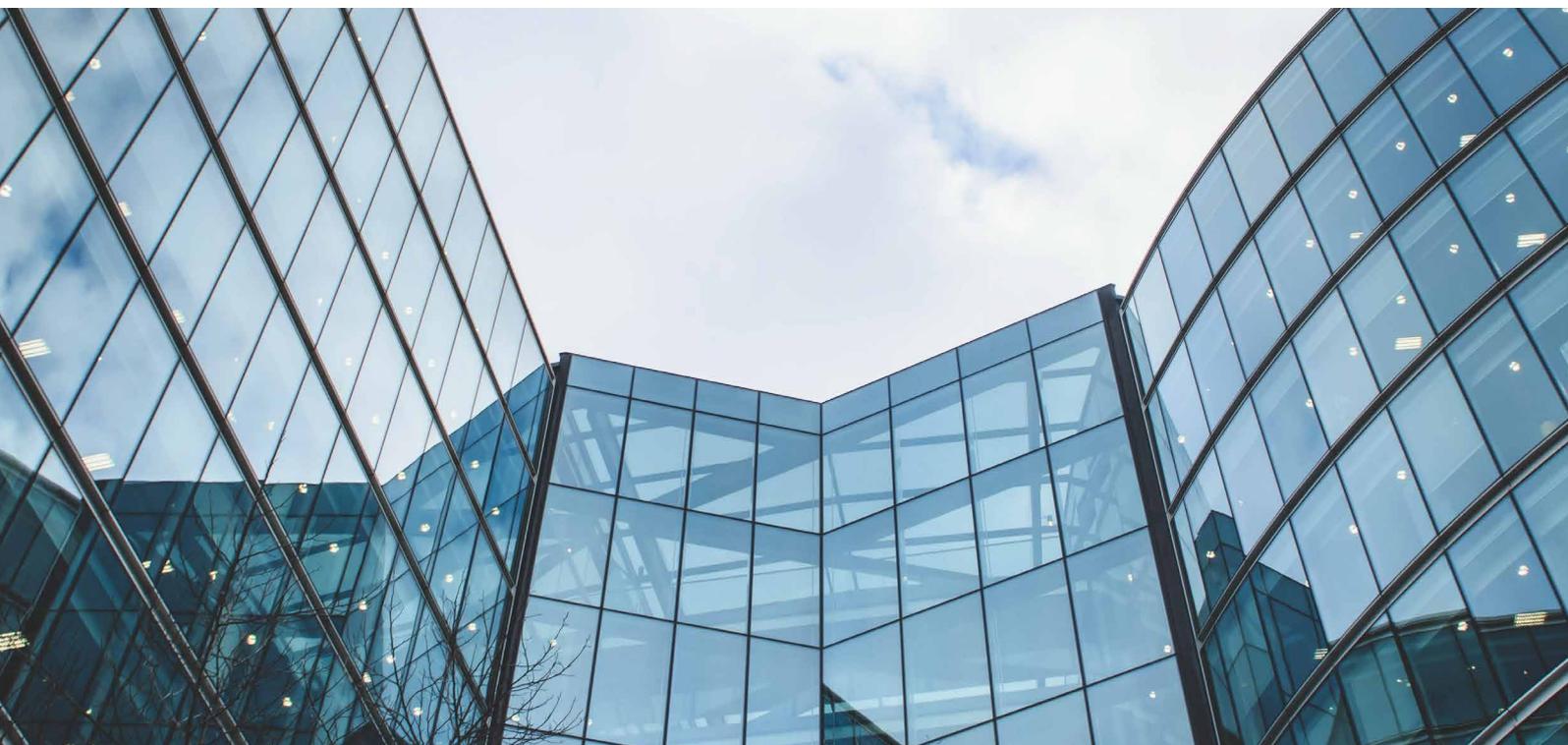
>80%



More than 80% don't conduct reputation due diligence on third parties such as distributors (81%) or potential M&A targets (86%)

Research methodology:

At the start of 2021, Kroll, in conjunction with the Association of Certified Fraud Examiners (ACFE) – Indonesia chapter, surveyed 241 fraud and risk professionals in Indonesia. A majority of the respondents belonged to the financial services sector (34.4%), followed by the public sector (29.5%). Respondents belonged to mid-to-high-level positions (more than six years of experience) and had responsibility for, or significant involvement in, determining their organization's risk management strategies.



Unreported Fraud: A Risky Blindspot for Indonesia

By Deni R. Tama, Managing Director, Forensic Investigations and Intelligence

The *Kroll/ACFE Indonesia Fraud Risk Survey* reveals that 62% of fraud incidents were detected through the whistleblowing system (WBS), which has been an effective fraud detection mechanism. This may indicate that the detection mechanism has done its job well. That's one way to see it. But this also means that we've been relying on a detection mechanism over which we have minimum control.

Proven high success rates but fraud still goes undetected

The WBS reports are loaded with leads, and in many instances, the whistleblower is even willing to testify, which makes the allegations easier to investigate. Indonesia's Corruption Eradication Commission's (KPK) sting operations (Operasi Tangkap Tangan – OTT) are good examples. Most of the intel used in OTTs are originated from the KPK's WBS (Pengaduan Masyarakat). Once a report is received, the commission sets up a surveillance operation in which phones are tapped, messages are intercepted and everything is monitored. When the colluding parties meet up to commit the fraud, they are arrested. With all the hard, direct evidence, the court can easily come to a decision. Hence, the KPK's conviction rate is almost 100%, which is good. But that doesn't answer the question about the unreported corruption cases.

The challenge with WBS

The problem with reactive controls like WBS is that it's reactive. After the system is installed and disseminated, all the organization can do is wait. Unfortunately, the system is not the only success factor. Many fraud incidents were never discovered because organizations operate in a culture that doesn't encourage whistleblowing. In many organizations, people who blow the whistle are considered disloyal or even traitors.

Most Indonesians, like other eastern societies, are brought up to appreciate seniority and to maintain harmony. And this is a challenge to any WBS in an organization, since our survey discovered that 83% of the fraud perpetrators in Indonesia are employees. With such a culture, employees would likely be silent on wrongdoings committed by their peers or management.

The statistics about WBS' performance tells us the portion of the incidents detected by WBS. It also tells us how dependent we are to the good faith of whistleblowers. But in an environment in which bribery is a common practice, for instance, we may not be so lucky. Nobody would bother reporting something that they themselves do. So instead of relying solely on reactive detection like WBS, we need to start implementing proactive detection systems.

Data analytics – it's only as good as the parameters

The vast development of IT has equipped us with the capability to search critical information in big data using data analytics (DA). DA is the process of analyzing datasets in order to identify trends and patterns and draw conclusions about the information they contain. Anti-fraud practitioners use DA to find suspicious activities in both transactional and static data. Judged by its name, DA may sound like an IT-heavy process. It is true that the procedure requires data processing skill and data processing applications. But unless you use this application with full machine learning capability (whereby human involvement is close to zero), the effectiveness of DA relies heavily on the parameters loaded into the system. A parameter is a set of logic that is based on certain typology of fraud and is used to filter transactions/activities. In essence, DA helps the management filter out activities/transactions that warrant further investigation.

Data analytics is no magic wand

Having said that, DA is not a magic wand. It would only be effective when implemented in an organization that understands its risks well. There is a myriad of possible ways by which an organization can be defrauded, and it is impossible to convert every possible fraud method into parameters, let alone to collate and process all the data. That would be too expensive and time-consuming. Bound by limited resources, organizations need to prioritize. This is where a fraud risk assessment process is critical. Fraud risk assessment is not rocket science, nor is it a new type of strategy in dealing with fraud. Indonesian banks would be familiar with the terms since it's one of Indonesia's Financial Services Authority's standard requirements in combating fraud in the financial services industry. As a matter of fact, this requirement has been around since 2011. By conducting fraud risk assessment, an organization can assess their fraud risk in a more systematic

manner. It helps the management focus on fraud risks that bring the most significant impact and are more likely to occur. Fraud risk assessment would also provide the organization with a tool to assess their readiness in mitigating the respective fraud risk.

Detecting unreported fraud – more proactive controls needed

Joseph T. Wells says in his book, "Corporate Fraud Handbook: Prevention and Detection," "Employees who perceive that they will be caught engaging in occupational fraud and abuse are less likely to commit it." Having an effective WBS is good, but we need more proactive detection controls, particularly because we operate in an environment that tends to appreciate harmony and avoid conflicts. As Wells pointed out, potential fraudsters would think twice if they know that WBS is not the only thing standing between them and a successful fraud scheme.

Contact

About Kroll

Kroll provides proprietary data, technology and insights to help our clients stay ahead of complex demands related to risk, governance and growth. Our solutions deliver a powerful competitive advantage, enabling faster, smarter and more sustainable decisions. With over 6,000 experts around the world, we create value and impact for our clients and communities. To learn more, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Kroll Securities, LLC (member FINRA/SIPC). M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Kroll Securities Ltd., which is authorized and regulated by the Financial Conduct Authority (FCA). Valuation Advisory Services in India are provided by Kroll Advisory Private Limited (formerly, Duff & Phelps India Private Limited), under a category 1 merchant banker license issued by the Securities and Exchange Board of India.