2020

Fighting fraud: A never-ending battle

Luxembourg in the context of PwC's Global Economic Crime and Fraud Survey

pwc

www.pwc.com/fraudsurvey

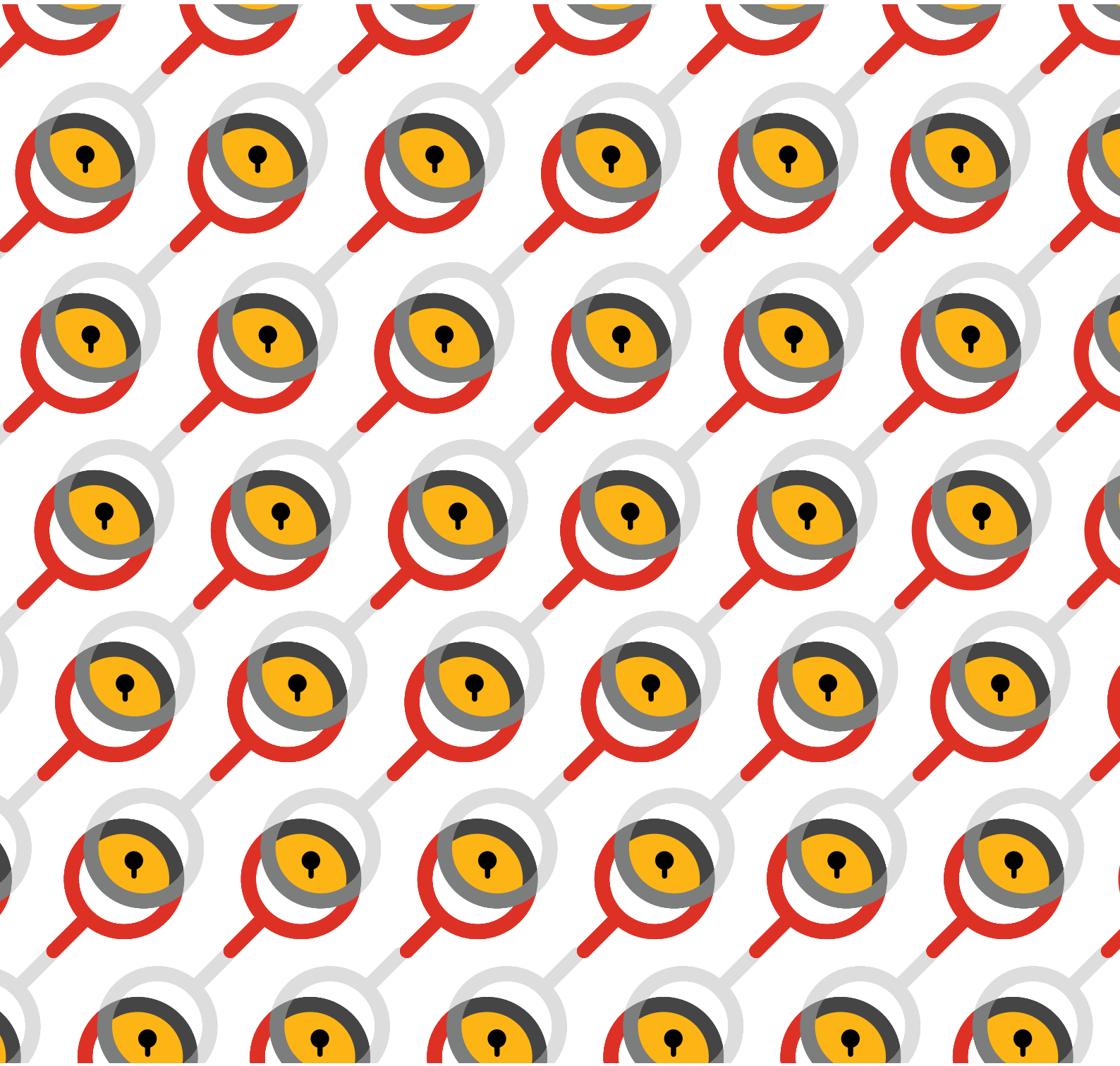
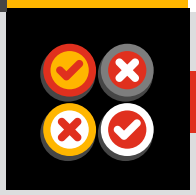
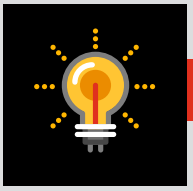


Table of content





Turn on the news or leaf through a newspaper and chances are you'll find a story about economic crime or fraud.

Bribery suspected in building collapse…Medical records and financial data of millions hacked… Corporate malfeasance to blame in product failure…Share price plummets as whistleblower alleges fraudulent accounting practices…Bank hit with multiple lawsuits over money laundering scandal...

Fraud and economic crime rates remain at record highs, impacting more companies in more diverse ways than ever before. Due to its status as a major international financial centre, Luxembourg is particularly vulnerable and has also seen its share of high-profile economic crime cases in the reporting period. With this in mind, we should consider:

Are we assessing threats and risks well enough… or are gaps leaving us dangerously exposed? Are the fraud-fighting technologies we have deployed providing the value we expected? When an incident occurs, are we prepared and, most importantly, are we reacting appropriately?

These are some of the provocative questions that lie at the heart of the findings of this year's Global Economic Crime & Fraud Survey. With fraud a greater, and more costly, threat than ever, it is essential to assess your readiness, deploy effective fraud-fighting measures and act quickly once it is uncovered.

Fraud

At PwC Luxembourg, we have a dedicated team of Financial Crime specialists that can help you provide innovative and advanced solutions to combat crime in areas such as:

- Asset Misappropriation
- Bribery and Corruption
- Customer Fraud
- Cybercrime and Data leaks
- Human Resources Fraud
- Market Abuse
- Money Laundering, Terrorist Financing and Sanctions
- Procurement Fraud
- Tax Evasion and Fraud

Our survey findings

When fraud strikes: **Incidents of fraud**

With nearly half of 5,000+ respondents reporting a fraud in the past 24 months, we have timely insights on what types of frauds are occurring, who is perpetrating the crimes and what successful companies are doing to come out ahead.

5,000+ respondents

62% of respondents were C-suite

72% have US$10M+ in global revenue

99 territories

US$42B in losses

47%

told us **they had experienced fraud in the past 24 months.** This is the **second highest** reported level of incidents **in the past 20 years.**

6 incidents of fraud

On average, companies reportedly experienced 6 incidents **in the last 24 months.**

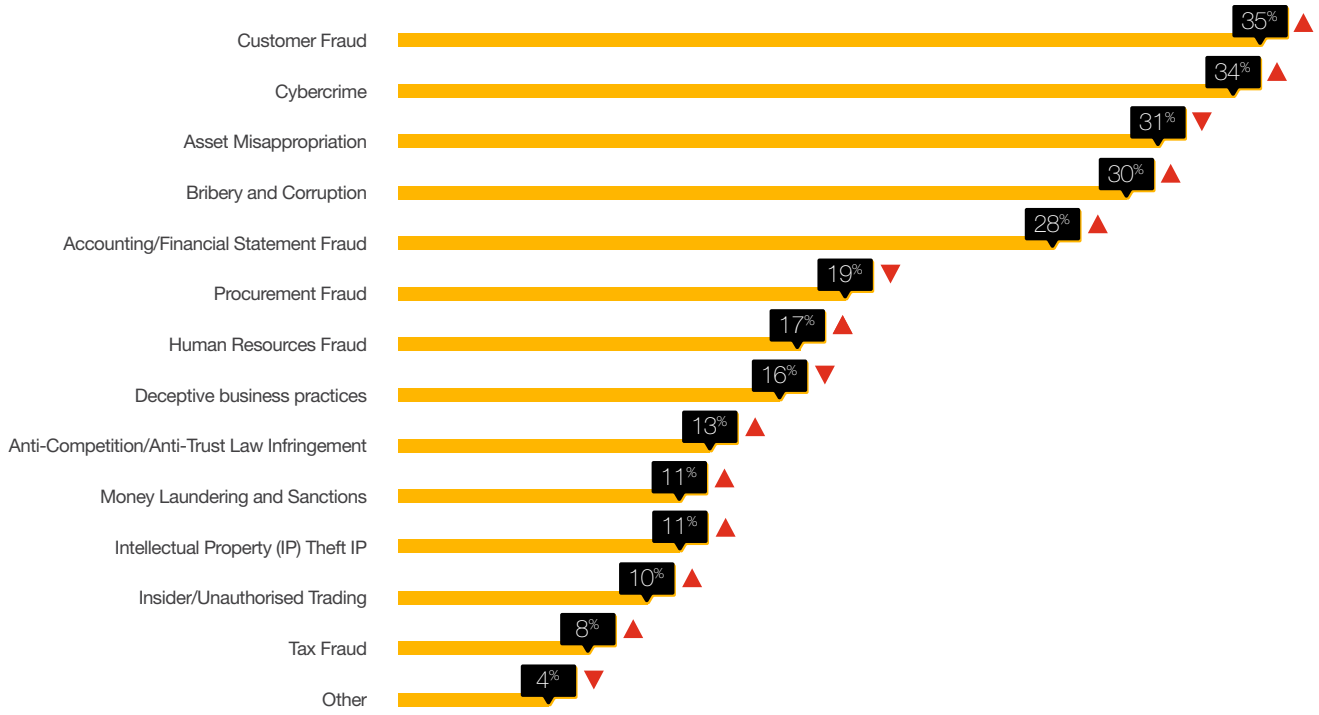
Top 4 types of fraud

1. Customer Fraud
2. Cybercrime
3. Asset Misappropriation
4. Bribery and Corruption

Reported incidents of fraud committed by customers, accounting fraud, anti-trust, human resources fraud, and bribery and corruption — saw big increases this year.

When fraud strikes: **Incidents of fraud**

Crimes: frequency of overall experience



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Most disruptive fraud events – by industry

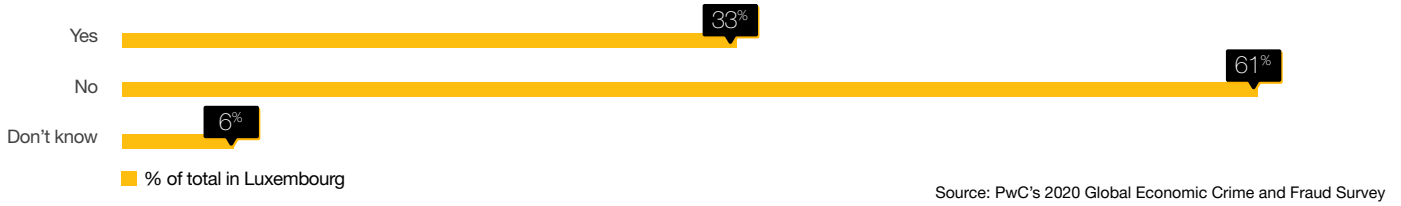
	Consumer Markets	Energy, Utilities & Resources	Financial Services	Government & Public Sector	Health Industries	Industrial Products & Manufacturing	Technology, Media & Telecommunications
1	Customer Fraud **18%**	Bribery and Corruption **17%**	Customer Fraud **27%**	Cybercrime **17%**	Cybercrime **16%**	Asset Misappropriation **21%**	Cybercrime **20%**
2	Asset Misappropriation **17%**	Asset Misappropriation **16%**	Cybercrime **15%**	Accounting/ Financial Statement Fraud **17%**	Accounting/ Financial Statement Fraud **13%**	Cybercrime **15%**	Accounting/ Financial Statement Fraud **16%**
3	Cybercrime **16%**	Accounting/ Financial Statement Fraud **13%**	Accounting/ Financial Statement Fraud **14%**	Bribery and Corruption **16%**	Customer Fraud **13%**	Bribery and Corruption **14%**	Customer Fraud **13%**

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Luxembourg perspective

Compared to 47% of global respondents answering they have experienced a fraud incident in 2019, the numbers for Luxembourg show a positive trend: only 33% (compared to 42% in 2018) of respondents say they have experienced fraud, corruption or other economic crime within the last 24 months. **Asset Misappropriation, Cybercrime and Money Laundering and Sanctions** remain the infamous top 3 of **the most pervasive economic crimes in Luxembourg.**

Has your organisation experienced any fraud, corruption or other economic crime in the last 24 months?



Source: PwC's 2020 Global Economic Crime and Fraud Survey

The overall decrease in reported fraud events can be partially attributed to robust investment in combating fraud, corruption and other economic crime as well as establishing dedicated programmes to address different types of economic crime.

However, many firms might not be aware of the economic crime risks they are facing (as evidenced by at least 6% that do not know about their fraud exposure), as several highly-publicised fraud cases in Luxembourg have shown in the past 24 months. In our Forensic Services and Financial Crime practice in Luxembourg, we have seen numerous cases and incidents that have occurred and been investigated in the past 24 months. Therefore, the current drop in the Luxembourg statistic to 33% seems at odds with our experience and public information. In any case, one in three survey participants has certainly been the victim of fraud or economic crime – which still represents a significant number. Moreover, many incidents likely go undetected and underreported, as economic crimes are often committed by internal perpetrators - especially senior management - which makes this misconduct particularly hard to detect.

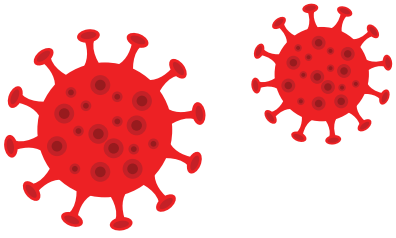
Luxembourg perspective

Focus on: **Fraud in times of COVID-19**

The numbers reported in this survey represent the situation before the outbreak of COVID-19 and show a different reality compared to the current situation. Our experience shows that **fraud is happening more often in times of crisis** as fraudsters are quick to adapt to new circumstances and try to use peoples' fear and sense of urgency to their advantage.

Therefore, we expect an increase in reported fraud cases in 2020, both at the beginning of the COVID-19 outbreak, but even more importantly, after deconfinement when companies and banks return step by step to "business as usual". This is when ex-post controls and audits of applications for financial aid might discover fraudulent payments, false information and fake beneficiaries. By then, recovering the money might prove difficult as the fraudsters will have used the time to move the funds far away from the prosecutor's searching eyes.

Several international and national authorities have already issued guidance to address the increased financial crime risks due to COVID-19. In Luxembourg, the CSSF has published the CSSF Circular 20/740 highlighting **key risks like Cybercrime, classic fraud, corruption in government support schemes, counterfeiting in the medical sector and insider trading** as new and emerging threats due to COVID-19. An increase of well-known fraud schemes can already be observed, such as phishing attacks with emails from supposedly trusted organisations like the WHO, fake suppliers offering products they never deliver or fraudsters demanding urgent payments and the circumvention of procedures to help with their alleged 'financial difficulties'. Fake or double applications for financial aid in times of COVID-19 are also expected.



The particular vulnerabilities in the financial sector that are identified in this context are:

- Online payment services
- Clients in financial distress
- Mortgages and other forms of collateralised lending
- Credit backed by government guarantees
- Distressed investment products
- Delivery of aid through non-profit organisations.

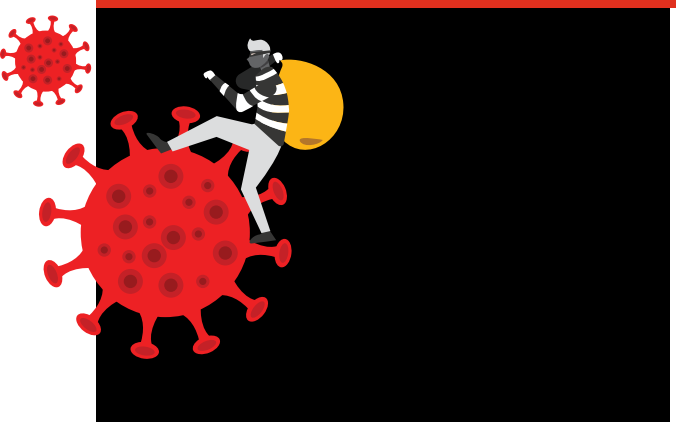
In a crisis it is particularly important to apply professional scepticism and question demands that do not make sense from a business perspective. Fraudsters try to target people specifically if they know that the targets are in the position to make a transfer or decision. When someone exerts pressure or even demands to disregard controls and procedures due to the urgency of the matter, all alarm bells should ring. Even if there is no time to perform additional controls – as organisations and people are struggling with the immediate challenges of keeping their business alive – standard procedures should always be followed: employees should be aware of the fraud risks, know who to turn to in case of suspicions and keep records of decisions and conversations as much as possible.

As **mitigating measures** the CSSF Circular 20/740 emphasises **efficient transaction monitoring, customer due diligence measures, AML/CFT business continuity and governance set-up, risk assessments and finally, proactive cooperation with authorities.**

Additionally, we would like to take this opportunity to recommend applying these **10 concrete fraud prevention rules** in order to decrease the impact of fraud related to COVID-19 and its aftermath:

1.	Respect the rules to check and validate payments, i.e. the separation of tasks between the person registering a payment and the person releasing the payment.
2.	Remember that the checks shall ensure that the money reaches the right person and isn't taken away by fraudsters.
3.	Perform additional checks in case an existing supplier wants to change its bank details, i.e. ask for a Relevé d'Identité Bancaire (R.I.B), and contact the supplier once again, using the contact information in your system, to confirm the change.
4.	Evaluate the legitimacy of new suppliers, for instance, by asking for their business permit or VAT number.
5.	Verify the quantity and quality of deliveries before carrying out payments.
6.	Consult with a manager or coordinator in case a supplier demands transfers to a country which is not its country of residence, or when unusual advances are requested.
7.	Pay special attention to emails from unknown external sources; contact the IT department in case of doubt.
8.	Question demands from individuals asking to speed up a well-established procedure; consult with the team or manager in case it's needed. In this regard, offer to call back the person. Including a colleague or coordinator when calling back is a smart idea.
9.	Refrain from performing any tasks like changes in the system or payments based solely on a call or email without additional proof.
10.	Check your treasury/financial situation daily in order to identify the disappearance of funds.

In case of suspicions, the detection of a fraud case or, an interest to improve fraud prevention and detection measures, our PwC experts are at your disposal to answer questions and advise on next steps.



Luxembourg perspective

Focus on: **Past Incidents of Fraud in Luxembourg**

Recent fraud cases in Luxembourg have shown that the problem may already be more widespread and persistent than suspected. In some cases, fraudsters have operated undetected and unbothered for years. The impacted sectors were mostly the financial sector; but fraud is also happening in the public and industrial sectors.

As per public sources, within the past two years, four organisations from the public sector have uncovered financial fraud in the form of embezzlement of public funds. In most cases, the alleged perpetrators appeared to be employees who circumvented normal procedures. Fraudulent activities included falsifying invoices, misusing official communication channels, and illegally transferring funds to unauthorised accounts. Often such schemes can go on for years before they are detected.

Any organisation who is a victim of fraud is usually revamping their procedures to avoid further incidents. In such cases it is always important to review and enhance internal controls. Even simple fraud prevention measures, e.g. a Code of Conduct or Anti-Fraud policy, can be effective in limiting fraud and saving costs in the long run. The general awareness about fraud risks remains a crucial element in any organisation but is still not always a given as these incidents show.

Focus on: **Financial Action Task Force (FATF) – Mutual evaluation of Luxembourg in light of the survey results and COVID-19**

The risk of Customer fraud and Cybercrime is especially high in Financial Services - the most important industry in Luxembourg. Another type of economic crime which is highly relevant for Financial Services is **Money Laundering**, which a third of our respondents in Luxembourg have experienced in the last 24 months and almost **15% named as their most disruptive fraud event experienced**. Money Laundering has of course received much regulatory attention in recent years, and as it is again Luxembourg's turn in 2020 to be assessed on its compliance with regards to the AML/CFT standards and recommendations set by the FATF, the regulatory focus has been further intensifying.

Due to the outbreak of COVID-19, the on-site visit of the FATF – initially planned for autumn of this year – will be impacted and the plenary discussion of the mutual evaluation report moved to October 2021. The latest procedures for mutual evaluations (updated in October 2019) foresee a period of 27 weeks between the on-site visit and the plenary discussion, meaning that the on-site visit could even be moved to early 2021.

However, this is no reason to relax. The overall context of the FATF evaluation is one of growing regulatory pressure. A number of revisions were introduced to the European AML/CFT framework, such as the 5th AML Directive (which Luxembourg had a slight delay in formally implementing into national law) and the 6th AML Directive (to be transposed by 3 December 2020). Moreover, the notorious series of large-scale money laundering scandals which spread across the whole of Europe during the reporting period put an additional spotlight on major compliance deficiencies in the European Banking system. In a so-called "highly-regulated" area like Europe, these scandals were at best embarrassing and caused additional pressure on regulators to prevent such occurrences from happening again. For instance, it triggered new approaches and discussions on pan-European AML regulatory approaches, e.g. through the EBA or ECB. Hence, the topic is hot, and AML will continue to be a focus area, as will Luxembourg.

Locally, we have already seen a steady increase in AML-related regulations for banks, asset managers, and insurers. This includes the publication of new CSSF circulars such as 18/698 and 19/730, and the publication of the national risk assessment and sub-sector risk assessments.

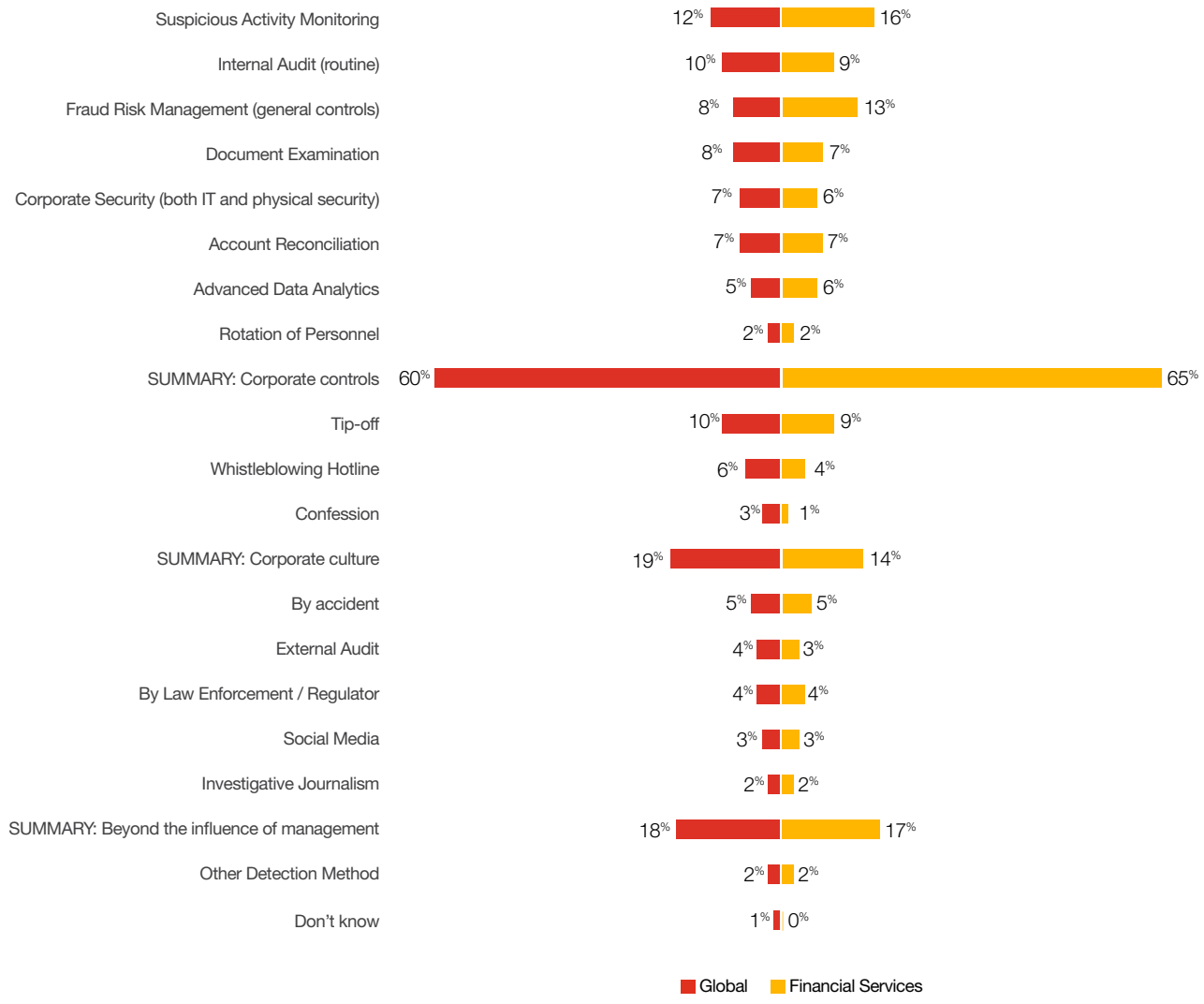
As the mutual evaluation process of the FATF is thorough and rigorous, and the on-site visit will include meetings and discussions for instance with relevant ministries and regulators, but also private sector representatives from financial institutions, now is the time to brush up on the latest regulatory developments in AML/CFT and check your compliance status. Preparation, as always, is key.

Detection of Incidents: **Detection methods**

Most incidents of fraud, corruption or other economic crime are detected through corporate controls, particularly through **Suspicious Activity Monitoring (12%) and Internal Audit (10%)**. Within the Financial sector, suspicious activity monitoring is especially important, with 16% of respondents saying that their most disruptive incident of fraud was detected through this channel, followed by Fraud Risk Management with 13%.

However, a significant percentage of fraud incidents is not detected through specific preventative or detective measures but rather through **tip-offs (10%)**, or even **by accident (5%)**, or other external sources, revealing the inadequacy of implemented controls and emphasising the need to raise awareness amongst employees to help them detect suspicious activities.

How was the most serious / disruptive fraud, corruption or other economic crime initially detected?



Source: PwC's 2020 Global Economic Crime and Fraud Survey

The Luxembourgish results are generally aligned with the Global FS perspective, as our country is involved with most participants from this sector. However, what is particularly striking is that, as in the past, the role of external and internal audit in the detection of fraud, remains very low and significantly below international results and may indicate an overreliance on computer control systems such as suspicious activity monitoring.

The internal audit function of organisations has a key role in monitoring and preventing fraud. This is often a top priority for internal audit teams, as a low detection rate might indicate a weakness in internal audit processes. Data analytics rank relatively low as an effective fraud detection tool in financial organisations. However, investigative analytics, using dedicated software solutions and tools, is a core element of PwC's forensic investigations approach. In our experience, it is crucial to most fraud cases: if applied properly at the prevention stage, it effectively improves crime prevention results.

When a potential case of fraud is detected, Luxembourg companies are likely to use internal resources to carry out an investigation – over 70% compared to 56% globally. And in most cases, companies reinforce their internal processes and procedures and/or conduct a training to prevent further incidents. Companies may ask for external help if they are lacking resources or expertise, but this step is not systematically followed in the industry. Yet, even a well-equipped company might not have the experience to deal with complex cases, especially when external reporting to law enforcement or regulators may occur. The biggest mistakes influencing the outcome of a crisis or incident investigation usually happen within the first hours or days. Official investigations can be hampered if the wrong decisions are taken during this period, or if potential evidence is corrupted due to untrained staff or inappropriate evidence collection.

One of the most important actions that an organisation can take is to ensure that everyone understands both the big picture of fraud risk management and how their own function fits into that picture. Many companies are establishing centralised fraud detection teams in order to gather information from sources such as whistleblowers, investigations, and system alerts, but also to trace the connections between the incidents for future investigations, compliance updates, and remediation. However, an enterprise-wide fraud function can create a false sense of security: one could think preventing and detecting fraud is someone else's responsibility. The first lines of defence in the business might not play up to their roles if they are not aware of their importance in fraud risk management. In addition, fraud can manifest itself in many different, ever-evolving and targeted forms, so every organisation should be cautious of 'one size fits all' solutions. Instead, a set up appropriate to every individual company is crucial.

Detection of Incidents: **Detection methods**

Focus on: **The Whistleblowing Directive (Directive (EU) 2019/1937)**

Whistleblowing did not feature significantly in the detection of incidents. Only 6% of respondents overall (4% in the Financial Sector) named Whistleblowing as the source of detection of the incident. This might also be because whistleblowing systems to report suspicions of fraud internally are not yet widespread.

This is set to change due to the **Directive (EU) 2019/1937 on the protection of persons who report breaches of Union law (Whistleblower Directive)** which has to be transposed into national law by 17 December 2021. The main goal of the Directive is to **strengthen whistleblower protection and make detection, investigation, and prosecution of breaches easier** through the mandatory establishment of internal and confidential reporting channels and follow-up procedures. This is particularly significant, as employees are often the first to recognise potential threats, suspicious behaviour of customers or colleagues, and shortcomings in rule enforcement.

At the same time, the Directive also aims to improve the reporting conditions and protection of whistleblowers against retaliation to **minimise the under-reporting of incidents**, as people might choose not to report suspicious activity or misconduct out of fear of the personal, professional and financial consequences.

The Directive covers breaches in many key areas of EU law, such as anti-money laundering and terrorist financing, consumer protection, public health, fraud, protection of the environment, and data protection. Legal entities both in the private and public sector with 50 or more employees (or more than 10,000 inhabitants in the case of municipalities) will have to establish channels and procedures for internal reporting and follow-up. Additionally, a competent authority in each EU Member State will have to be designated to introduce an additional external reporting channel.

It is still too early to gauge the full impact and benefit of the Whistleblowing Directive, as we have to wait for the national transposition into Luxembourg law, in any case, many employers will face the requirement to implement new processes.

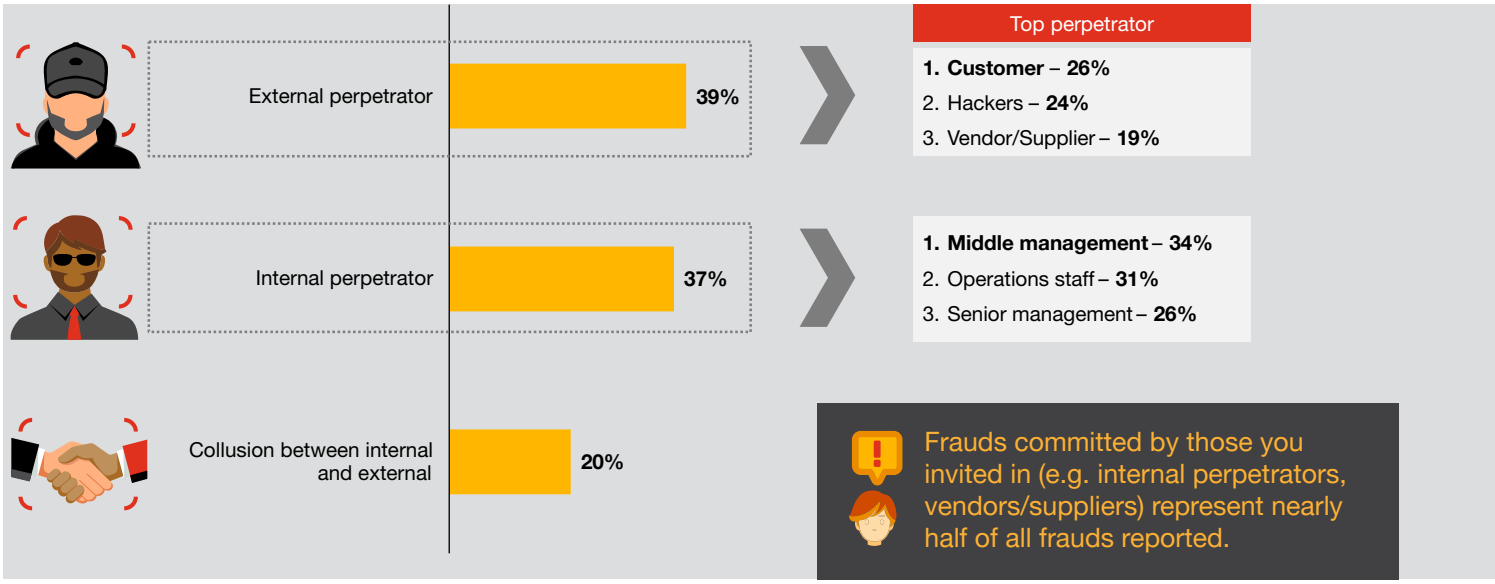
Nearly half of reported incidences **resulting in losses of US$100 million or more were committed by insiders.**

Source: PwC's 2020 Global Economic Crime and Fraud Survey

The perpetrators: **Who's committing fraud**

Fraud hits companies from all angles – the perpetrator could be internal, external, or in many instances there will have been collusion. Business partners remain a risk and fraud committed by management is trending upward.

Perpetrators: external, internal and collusion between them



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Customer Fraud (26%). Fraud committed by customers tops not only the list of external perpetrators (at 26%) for the most disruptive fraud, but also the list of all crimes experienced (at 35%, up since 2018):

- Not surprisingly, customer fraud is especially prominent in the Financial Services and consumer markets sectors. This could be significant, as more industries shift to direct-to-consumer strategies.
- The good news? It's also one of the frauds where dedicated resources, robust processes and technology have proved effective for prevention.

Although consumer fraud is the biggest global threat, it remains currently underrepresented in Luxembourg, since it is rather a direct B2C or retail-focused risk. The nature of the Luxembourg market makes customer fraud therefore less relevant than in large countries. However, the evolution and digitalisation of distribution channels might make this a topic of interest for Luxembourg in the future.

Third parties (19%). More and more, companies outsource non-core competencies to contain costs. But these business partners can be fraught with risk – a risk many companies have not formally addressed:

- One in five respondents cited vendors/suppliers as the source of their most disruptive external fraud.
- But half lack a mature third-party risk programme - and 21% have no third-party due diligence or monitoring programme at all.

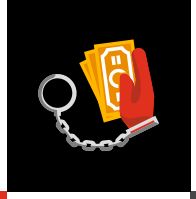
In contrast, the level of sophistication of third-party due diligence is higher in Luxembourg. 51% have at least a documented, risk-based due diligence and ongoing monitoring process for third parties and 13% use web-based applications and other tools and technologies. Only 10% admit to having no due diligence process at all. This reflects the high concentration of financial services in Luxembourg that are subject to strict local or EU regulations.

Senior management (26%). These crimes are often among the most insidious because of the ability top executives have (whether through delegated authority levels, system knowledge, or influence) to override – or conspire to override – internal controls. In cases that we see in Luxembourg, the perpetrators are often long-term and experienced employees with some degree of managerial status or influence. Fraudsters of this type are particularly dangerous, since they are typically well trusted and very knowledgeable about weaknesses that can be exploited.

Accused of fraud? This year, for the first time, we asked respondents if their organisations had been accused of perpetrating a fraud. Of those who reported experiencing fraud, nearly 3 in 10 were also accused of committing a fraud, corruption, or other economic crime:

- In almost equal numbers, competitors, regulators, employees, and customers were most likely to point the finger.
- Enhanced regulatory focus, and in some territories, whistleblower incentives, may contribute to this trend.

In Luxembourg, only 5% of respondents said they were accused of fraud, corruption, or other economic crime. This is a much lower percentage than reported globally. Many of the accusations seem to come directly from the regulator and related fines or administrative sanctions have grown in the past but still remain lower compared to large jurisdictions like the US or UK. Still from a local perspective they hurt since organisations are much smaller and regulators are continuing to increase the pressure.



Feeling the impact: **The cost of fraud**

Fraud losses are complex. The costs of direct financial loss or costs due to fines, penalties, response, and remediation can easily be tallied. But some costs are not easily quantified, including brand damage, loss of market position, employee morale and lost future opportunities.

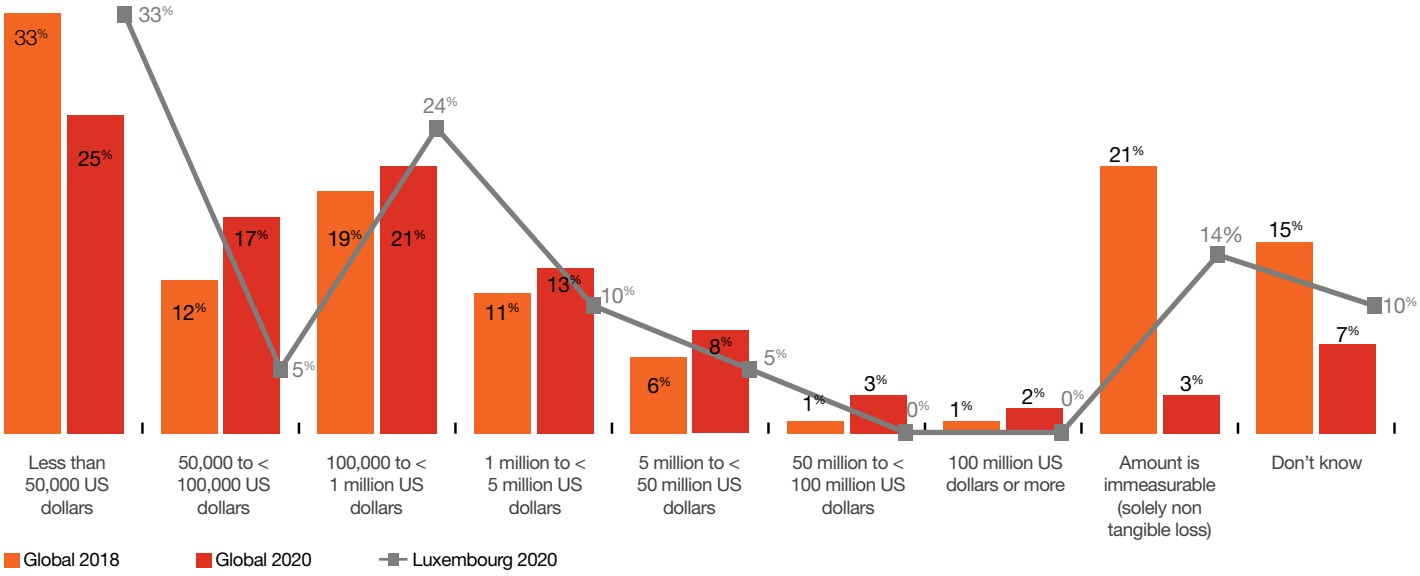
Some frauds, such as external frauds, generally strike from outside the company, are transactional in nature, lend themselves to active monitoring, and when managed properly may reduce financial impact. For other frauds like bribery and corruption, or those internally perpetrated, it is important to manage and mitigate the downside risk. These frauds tend to be harder to predict and monitor, and result in more costly fines. They also have ancillary repercussions such as lost business or brand harm.

Roughly **13%** of respondents globally who experienced a fraud in the last 24 months reported **losing more than $50 million across all incidents.**

Top 5 costliest frauds. Antitrust, insider trading, tax fraud, money laundering, and bribery and corruption were the top causes of direct losses — sometimes compounded by the significant cost of remediation and after-the-fact fines.

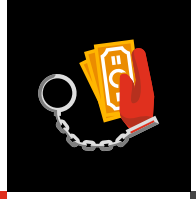
Major frauds perpetrated by insiders are potentially far more damaging than externally perpetrated crime and not just because the financial loss is likely to be higher. 43% of reported incidences resulting in losses of US$100 million or more were committed by insiders. But such crimes can also often result in civil or criminal actions against the company and those involved, as well as reputational harm, management distraction and loss of business.

Direct financial loss due to economic crime is on the rise



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Most of the cases in Luxembourg caused less than $50,000 in damages. However, we observe an **increase in the direct monetary loss due to economic crime**, globally as well as in Luxembourg: Compared to the numbers in 2018 there is a shift towards a higher financial impact due to economic crime incidents. Even if these do not happen very often in absolute terms, their impact is huge, and they will likely happen again – even in Luxembourg. And if it happens to an organisation, the impact is usually heavy and should never be underestimated.



Feeling the impact: **The cost of fraud**

Focus on: **Diving in**

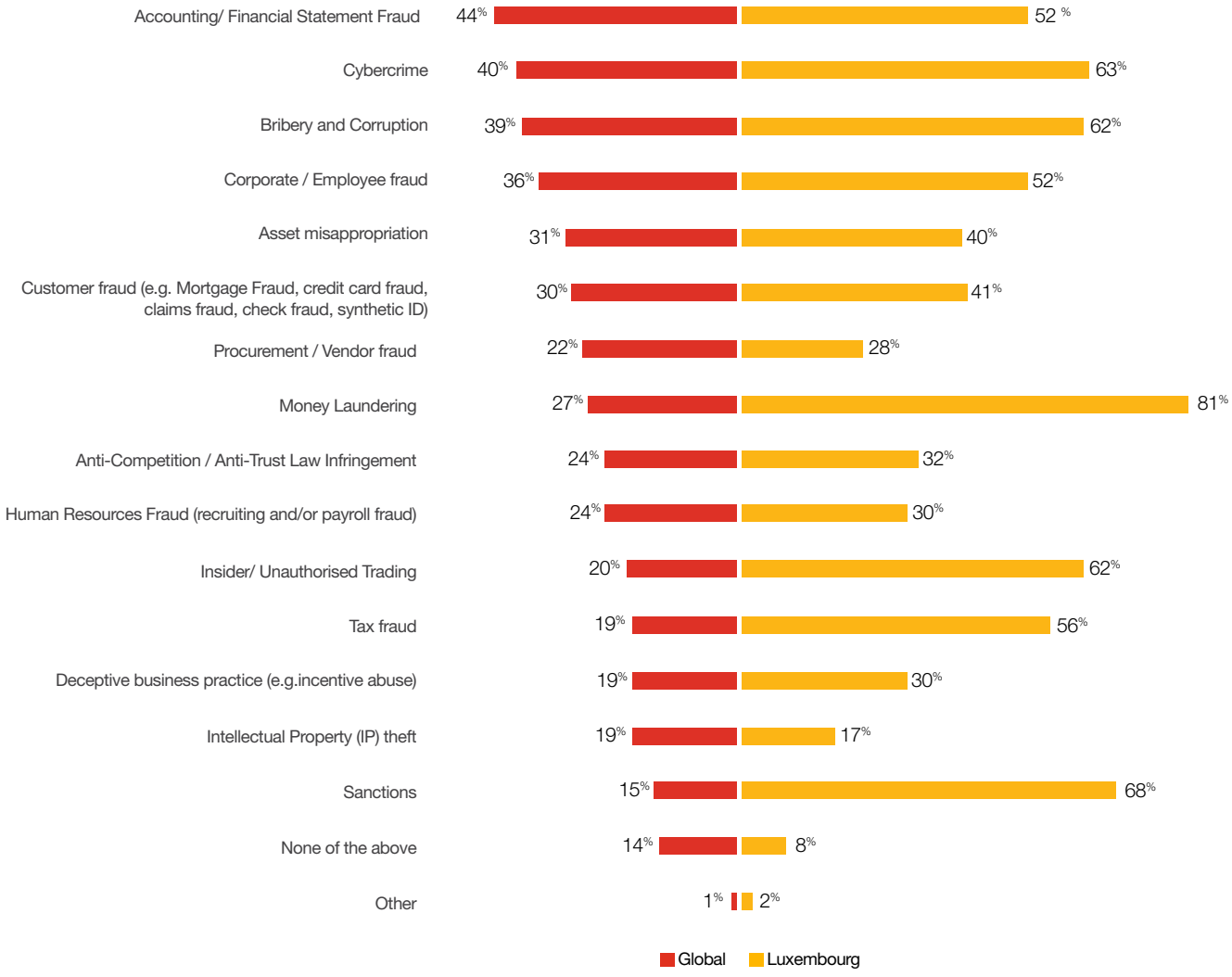
Bribery and corruption remain a big challenge. One third of all global respondents say they had either been asked to pay a bribe or had lost an opportunity to a competitor whom they believed had paid a bribe. In contrast, less than 5% of the respondents in Luxembourg said they were asked to pay a bribe or believed they had lost an opportunity to a competitor. Bribery and corruption are nonetheless important topics in Luxembourg, as the money flows linked to corruption passing through our financial sector constitute a predicate offense for money laundering and hence, are highly relevant for Luxembourg. The topic also remains relevant due to the impact of extraterritorial international anti-corruption laws, such as the UK Bribery Act, U.S. FCPA, and Sapin II in France to name a few.

Among the responses, there were a few **blind spots and surprises:**

- **Globally, 6 in 10 organisations – in Luxembourg, 4 in 10 organisations – do not have a programme to address bribery and corruption risk.**
- Nearly half of all global respondents either do not perform a risk assessment, or only perform an informal one, compared to a third of respondents in Luxembourg.
- Half of all global respondents either do not perform or perform only informal risk-based due diligence and on-going monitoring of third parties — despite the fact that third parties represent one of the greatest bribery and corruption risks. The numbers for Luxembourg are somewhat stronger, with only 36% saying they have no or only informal controls on third parties.
- Fewer than 3 in 10 companies perform limited testing of the operating effectiveness of their controls, and another 12% do no testing at all. Only 5% of the respondents in Luxembourg admitted to no testing at all.

As most respondents in Luxembourg operate in the financial sector – which is highly regulated – the more favourable numbers for our country are not surprising. Many respondents already have processes and controls in place to prevent economic crime, in particular, regarding money laundering and sanctions, and cybercrime. However, we still observe shortcomings, and it is important to stay vigilant and up-to-date on new developments and regulatory requirements. Last but not least, it is also important to determine whether the implemented programmes are working effectively.

Does your organisation have a dedicated programme to address any of the following risks?



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Taking action: **Being prepared**

What are you doing to prevent and identify fraud? What programmes, methods, and technologies are working — and which ones are not? What perception gaps are still standing in the way — and what opportunities for improvement are ripe to be seized?

Fighting fraud pays… but are you doing enough? On average, companies have four dedicated programmes in place to mitigate fraud risk (larger companies with more than 10,000 employees average more). While nearly two-thirds of companies reportedly have policies and procedures in place and the majority (6 in 10) include training and monitoring — **barely half of organisations are dedicating resources to risk assessment, governance, and third party management.**

So what actions are most effective?

1. **Identify, rank and address all your risks.** Companies should perform robust risk assessments, gathering internal input from stakeholders across the organisation and across geographies, to identify risks and assess mitigating factors. These assessments should also incorporate external factors. There is a wealth of information available in the public domain, and ignoring it could potentially result in a big miss. Risks should be assessed at regular intervals (not through a 'one and done' approach).
2. **Back-up your technology with the right governance, expertise, and monitoring.** Recognise that one tool won't address all frauds – and technology alone won't keep you protected. Technology is often only as good as the expert resources, data management and visibility, robust controls, and regular monitoring dedicated to it.
3. **Take notice.** The ability to react to a fraud once it is identified is critical and a key element of an effective fraud program. The ability to quickly mobilise the right combination of people, processes and technology can limit the potential damage. Disruptive frauds often disguise a strategic inflection point – triggering the opportunity for broader organisational transformation.

Technology is just part of the answer

Large numbers of organisations have invested heavily in new tools and techniques in recent years, but many respondents revealed concerns about deploying technology:

- Fewer than **3 in 10 (for Luxembourg fewer than 2 in 10) strongly agree** that they have been able to implement or upgrade their technology — with issues of cost, limited resources, and lack of systems cited as obstacles.
- Considering alternative technologies and techniques, only 25% are using artificial intelligence (AI) — a technology that is ever more prevalent today (however, nearly 40% of the organisations using AI are struggling to find value in it as a fraud-fighting tool). The numbers in Luxembourg, however, for the use of AI are particularly low with just 3% of respondents using AI and almost 50% saying they have no plans to use AI.

Compared to the global numbers, Luxembourg still seems relatively averse to the use of alternative/disruptive technologies and techniques. The notable exception is transaction monitoring, which is wide-spread in Luxembourg, mainly due to regulatory requirements to detect unusual activities that might suggest money laundering. More than 65% of the respondents in Luxembourg are using transaction monitoring, however, of those using it 17% are not finding it valuable. This might be due to the use of off-the-shelf tools which are not adapted to individual business models and therefore provide only limited effectiveness.

Consequently, this is an area where the most progress could be made to upgrade organisations' defence mechanisms. This could be complemented by more guidance from regulators, e.g. including how to improve transaction monitoring systems in the financial sector, or what to implement with regards to asset screening as one of the hot new topics that the asset management industry is currently dealing with.

Highly-regulated sectors need to place an increased focus on fraud and other economic crime. As companies face an ever-increasing stream of complex data and regulatory requirements, bringing in external forensic experts to analyse and streamline internal processes, and to handle routine investigations can help, in addition to decreasing the legal and consulting costs in the long run.

A single tool or technology alone cannot constitute an entire anti-fraud programme. Are you collecting the right data with the right rules and requirements? How are you analysing that data? Are you feeding findings back into your programme to make it more robust? As companies struggle to implement new anti-fraud technologies, organisations using new tools such as artificial intelligence do find value when implemented appropriately.

Taking action: **Being prepared**

Focus on: **Transaction Monitoring**

Financial institutions in Luxembourg must monitor thousands of transactions each day and most of them rely on an automated transaction monitoring system to detect suspicious activity, e.g. relating to money laundering and terrorist financing. However, **a monitoring system can only be effective if it is tailored to the specific nature of the business and the customer base** of each institution and uses appropriate volume and frequency rules to provide the best results.

Transaction monitoring, from a Luxembourg perspective, strongly depends on the scale and nature of the transactions being different between banks or investment funds. Furthermore, the majority of the transactions occur cross-border, making transaction monitoring scenarios more complex. The default scenarios often suggested by software vendors do not always meet the Luxembourg market requirements sufficiently, and here more regulatory guidance could be helpful and CSSF has already announced a dedicated Circular on transaction monitoring.

The amended AML law (Law of 12 November 2004 on the fight against money laundering and terrorist financing) highlights only the need to monitor high risk transactions more diligently, without going into more detail. However, this lays the foundation regarding the direction in which transaction monitoring will develop. With an increasing focus on the effectiveness of transaction monitoring systems it is also important to **stay up-to-date on the methods that are used to launder the proceeds of criminal activities** – the FATF regularly publishes typologies for different industry sectors – and to **regularly update the system and test its effectiveness.**

Focus on: **Asset Screening**

With the publication of the **CSSF Circular 18/698**, asset screening has become a new focal point of regulatory attention in Luxembourg as IFMs must now apply due diligence measures on the assets of the UCIs they manage.

It can be safely expected that the regulatory onus on IFMs in general and asset screening in particular will continue to increase. On the one hand, the ML/TF Sub-Sector Risk Assessment on Collective Investments – published in January 2020 by the CSSF – identified a high-risk for money laundering in the Collective Investments Sector. And on the other hand, the CSSF also identified the lack of consideration of the investment sides (assets) within the Risk Based Approach as one of the most common shortcomings and recommended to account for the ML/TF risks represented by the investments within the funds' risk scoring.

To meet the requirements of the CSSF, Portfolio Managers should therefore be sure to apply **risk-based due diligence measures on their investments** – which requires an understanding of the risk represented by the specific assets – and **screen them against the relevant financial sanctions lists**. It is also important to understand and assess the roles of the various related parties involved with the assets in which the IFM's are investing. With only limited guidelines available and no market standard yet established, our experienced AML subject matter experts can help you navigate your regulatory obligations.

Responding: **Doing the right thing**

What do you do when your organisation is hit by fraud? **Nearly 60% of companies who conducted an investigation ended up in a better place** — but nearly half of respondents did not conduct an investigation at all. And barely one-third reported it to their board.

Regulators — and increasingly, the public — demand more. Reacting too slowly can not only cause more immediate damage, it can cascade into a broader crisis. **According to PwC's Global Crisis Survey**, organisations with 5,000 or more employees are most likely to experience crises related specifically to **cybercrime (26%), natural disaster (22%), leadership (17%) or ethical misconduct (16%)**, including fraud, corruption, and corporate malfeasance.

According to PwC's 2020 CEO Survey, 58% of CEOs are concerned with their readiness to respond to a crisis

What key steps did organisations that emerged in a better place take?

Conduct an investigation (71%). Getting to the root of the problem is key to preventing further damage. Companies often seek external assistance to investigate fraud when either objectivity is crucial, or they lack the resources or expertise to do it themselves. A forensic accountant / specialist can be especially useful in detecting potential weaknesses and malpractice in internal processes and controls.

Bolster internal controls, policies and procedures (>50%). While some policies and procedures may be easy targets, it is important to assess operations globally and identify what might be missing.

Take disciplinary action against employees (44%). In line with regulatory guidance, compliance programmes should apply to all and no-one should be beyond their reach; no person should be deemed too valuable to be disciplined. Enforcement of a compliance programme is one of the keys to its effectiveness.

Only **56%** of organisations **conducted an investigation** of their worst incident

Barely **one third reported it to the board**

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Almost 90% said they experienced negative emotions after an incident of fraud

42%
positive feelings and emotions

89%
negative feelings and emotions

Source: PwC's 2020 Global Economic Crime and Fraud Survey

Disclose the incident to government authorities (37%) and to the auditors (27%). Disclosing the fraud early can sometimes result in a more favourable outcome with regulators. In the financial sector, it is particularly important to adhere to reporting requirements and to consider as well whether the auditor needs to be informed about the incident. Obviously, this implies proper involvement of the Board of Directors, but it is surprising to see that this is not systematically the case. In a highly-regulated market like the financial sector, this is an absolute prerequisite.

Conduct training (32%). Training does not only better inform staff of new policies and procedures, it also promotes a stronger culture around fighting fraud.

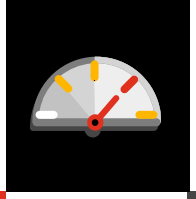
Not surprisingly, respondents overwhelmingly (**89% to 42%**) said they experienced negative emotions after an incident of fraud. However, those who stated their organisation was in a better place post fraud stated:

- the main perpetrator was external to the organisation ('we were attacked'), rather than internal ('one of us') (**48%**).
- companies felt strongly that they stayed true to their values, acted as a team and prepared and followed a plan.

Taking stock

Nobody wants to fall victim to (or worse, stand accused of) fraud. But there's another way to look at a major disruptive event: as an inflection point, a possible trigger to organisational transformation. Whether that transformation is negative or positive — a full-blown crisis, or an improved market position for example — depends on how well the business was prepared and how it was managed.

The data shows that there's a significant upside to taking stock when an incident strikes. **Nearly half (45%) of all global respondents who have experienced a fraud say they emerged in a better place** — citing attributes such as an enhanced control environment, streamlined operations, fewer losses, and improved employee morale. Large companies are even more likely (52%) to say they emerged better off – citing adoption of new technology and fewer repeat incidents, in addition to a better environment and streamlined operations.



Emerging stronger: **Measuring success**

People in fraud-related functions often find themselves fighting for an increased budget, in order to invest in new technologies, implement new programmes or hire additional resources. In addition, **nearly 40% of our global respondents, but only 30% of our Luxembourg respondents, say they plan to increase spending on fraud prevention in the next two years.** But do the measures work? Will they see a return on their investment? And how do you justify the expense to your leaders?

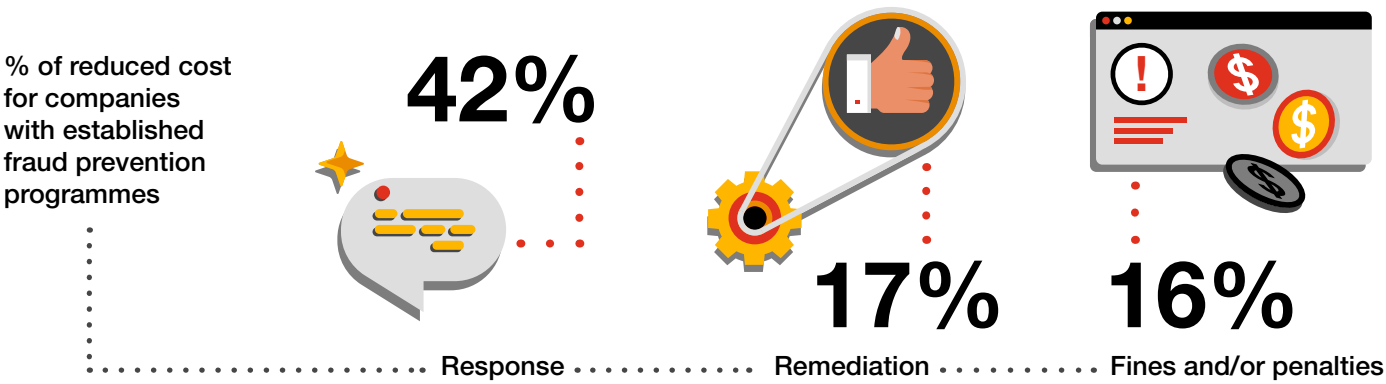
It can be challenging to quantify the benefits of a fraud-fighting tool. It's common sense that effective fraud prevention measures reduce the quantity and magnitude of future fraud. But here's a more interesting statistic – **there is a clear link between fraud prevention investments made upfront and reduced cost when a fraud strikes.**

Companies that have a dedicated fraud programme in place generally spent less (relative to revenue) on response, remediation, and fines:

- Companies with a dedicated fraud programme reportedly spent 42% less on response and 17% less on remediation costs than companies with no programme in place.
- Where bribery or corruption was experienced, companies with a dedicated bribery and corruption programme spent 58% less on remediation than those without.

The results for Luxembourg are below the global benchmark and this might be one of the explanations for the low score on the use of technology. This is certainly an area with room for improvement if we want to be on par with the global trends. Since finance is the most important sector in Luxembourg, it will also be interesting to follow how the regulatory agenda will push this topic into the market, based on the European regulatory framework. Transaction monitoring and Asset Screening have already been mentioned above as two key areas in this context.

Companies who invested in fraud prevention incurred lower costs when a fraud was experienced



Source: PwC's 2020 Global Economic Crime and Fraud Survey

Once a programme is in place, periodic assessment and refinement are key elements for the following reasons:

- Business models are often dynamic and can evolve or change before risk programmes are established or enhanced, leaving companies exposed to unanticipated risks.
- There's increasing convergence in certain industries — for example, technology companies offering financial services, or health companies entering consumer markets —and risk management programmes need to be adapted to meet those new or evolving risks.
- A hotline call or audit finding may yield a risk previously not considered.

And perhaps most importantly, regulators are paying more attention to compliance programmes. Some of them are starting to request evidence showing that compliance programmes are effective.

Many regulators recognise that compliance programmes should be risk-based and right-sized and that no programme can catch all improper activity. There is no cookie-cutter approach to compliance, and a programme at a large telecommunications company will no doubt look different than a program at a small retailer. Even so, both may be adequate in addressing the particular risks each organisation faces.

Similarly, there is no single prescribed method for assessing effectiveness. There are many scholarly articles on assessing the effectiveness of training that provide helpful insights; however, not much is available on assessing the effectiveness of a third-party management programme, for example.

This provides an opportunity for companies to define their own meaningful assessment system, which may cover areas such as: vendor rationalisation statistics, vendor rejection statistics, participation of vendors in training programs, vendor certifications, and/or a reduction in exception rates /or less findings during third party audits. The key is to have a defensible measurement in place that will help to demonstrate that the programme area has been tested and how it would prevent or detect problematic misconduct in the future.

In conclusion

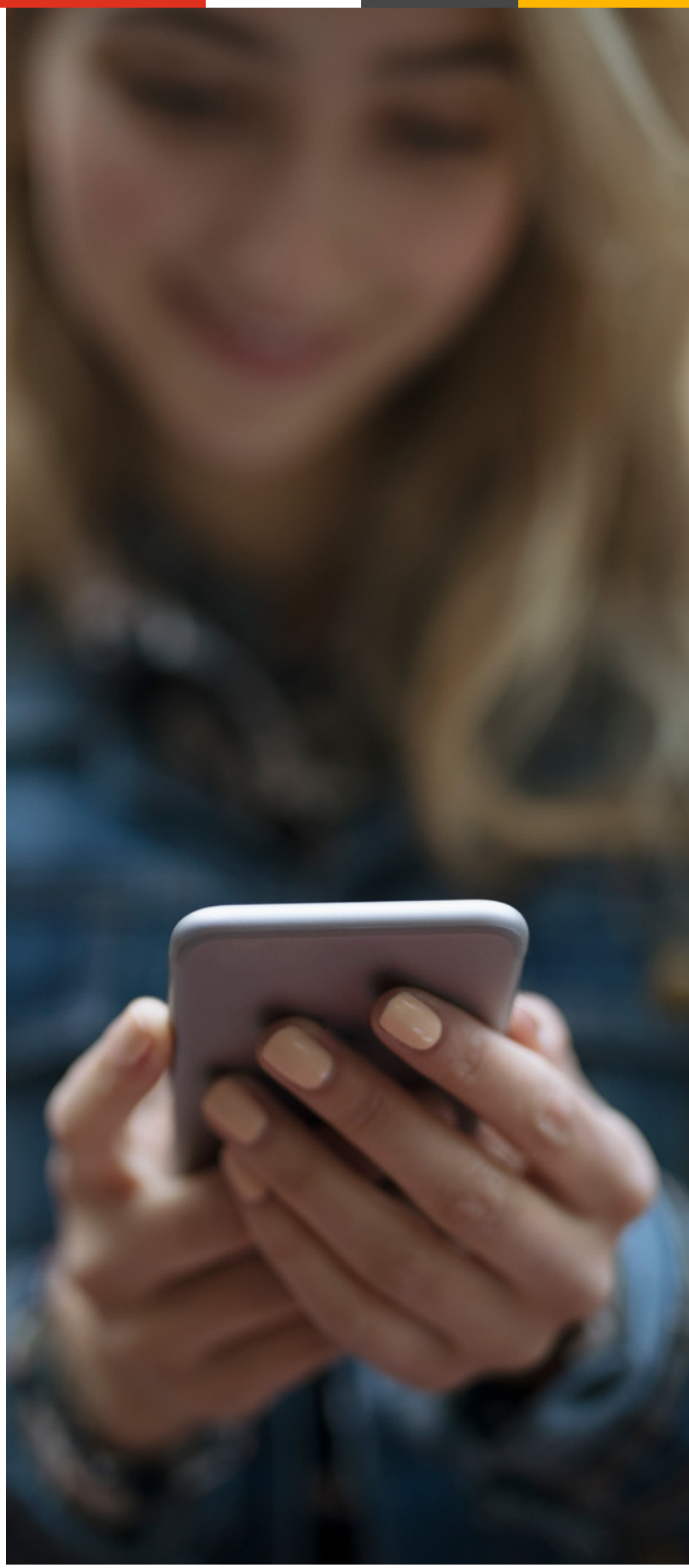
So where do you stand? Are you a leader in preventing, detecting, and responding to fraud? Or are there areas for improvement that you should address as a matter of urgency?

Either way, you need to act. Even the 'best' anti-fraud programmes need to be continually assessed and refined. As we have seen, the perpetrators and methods of crime evolve, so your defences must also be modified to meet the new risks.

Alternatively, if your fraud defences have blind spots or gaps, you are leaving yourself exposed to risks and the increasing costs of fraud.

Fraud is a risk to which no business is immune. And when hard questions are asked after an incident, a lack of awareness or insight is no excuse.

Now is the time to understand just how prepared you are. Our team can help you anticipate fraud and prevent a crisis or be by your side to find out what really is happening when you suspect the worst. Our forensic investigators, accounting professionals, computer forensic specialists, engineers and other experts can support you in investigating, analysing and resolving a potential crisis as well as advise you on steps you can take now to combat fraud in the future.



To learn more

Want to gain a better understanding of your fraud and financial crime risks and know more about what you can do in the fight against fraud?

Contact one of our subject matter experts

Forensic Services, Financial Crime & AML

Michael Weis

Partner, Forensic Services & Financial Crime Leader
PwC Luxembourg
+352 49 48 48 4153
michael.weis@lu.pwc.com

Anti-Money Laundering

Roxane Haas

Partner, Banking Leader
PwC Luxembourg
+352 49 48 48 2451
roxane.haas@lu.pwc.com

Birgit Goldak

Partner, AWM & Distributor Due Dilligence
PwC Luxembourg
+352 49 48 48 5687
birgit.goldak@lu.pwc.com

Insurance

Anthony Dault

Partner, Insurance
PwC Luxembourg
+352 49 48 48 2380
a.dault@lu.pwc.com

Tax

Murielle Filipucci

Partner, AML Tax
PwC Luxembourg
+352 49 48 48 3118
murielle.filipucci@lu.pwc.com