COVID-19 CONTENT SERIES

A BLUEPRINT TO MANAGING CORPORATE FRAUD RISK DURING A PANDEMIC

By Nelson Luis, MBA, CFE, CFI

The Institute of Internal Auditors
INTERNAL AUDIT FOUNDATION
FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS

Table of Contents

About the Expert

Nelson Luis, MBA, CFE, CFI

Nelson is a Principal with EisnerAmper LLP's Forensic, Litigation and Valuation Services Practice. He has extensive global experience advising clients on complex domestic and cross-border forensic and litigation support matters. Nelson has managed 150+ cross-border investigations in 40+ countries, including in nearly every Latin American country, Asia-Pacific, and Africa. He is a member of the IIA Philadelphia Chapter and the recipient of the *Philadelphia Business Journal's* Minority Business Leader Award for efforts in the forensic accounting services industry.

FOREWORD

The risk of fraud is present in all organizations to a greater or lesser degree, depending on various internal factors (organizational culture; level of maturity in corporate governance, risk management, and internal control; type and size of business; etc.) and external factors (industry; national/regional context; market in which it operates; etc.). Unfortunately, fraud is a risk that can affect any organization at any time — in normal times and in times of crisis. Furthermore, in times of crisis, the risk of fraud may increase, as some people may find a reason (pressure/incentive), an opportunity (chance), or a justification (rationalization) to commit irregularities.

In times of crisis, such as the current COVID-19 pandemic (a health crisis that also generated a social and economic crisis), some people may decide to commit fraud for the first time. Those who are accustomed to committing fraud may also try to take advantage of the circumstances to commit new or greater irregularities. Committing fraud at any time is reprehensible, but even more so when it is committed in times of crisis, even sometimes by appropriating resources intended to help overcome the crisis.

As a contribution to the global fight against fraud and corruption, the Latin American Foundation of Internal Auditors (FLAI) decided to sponsor this report, *A Blueprint to Managing Corporate Fraud Risk During a Pandemic*, produced by the Internal Audit Foundation. Author Nelson Luis offers a practical approach to directly address the scenario of an increased risk of fraud (corruption, misappropriation of assets, fraudulent financial statements) in organizations due to the pandemic. He considers related key actions, including assessment of vulnerabilities, risk mitigation, and monitoring fraud alerts (red flags).

This report also presents very useful analysis on how to face a possible increase in the risk of fraud in these times of COVID-19 (pre- and post-pandemic) from the perspectives of the fraud triangle, the three lines model, cybersecurity, and global risk. People and organizations around the world are fighting to overcome the crisis caused by the COVID-19 pandemic and its direct and collateral effects. In this fight, internal auditors are actively helping organizations overcome and recover from the crisis.

FLAI, let's move forward together!

Regards,

Jorge Badillo, CIA, QIAL, CRMA, CCSA, CGAP, CISA
Chairman of the Board
Latin American Foundation of Internal Auditors (FLAI)

INTRODUCTION

The COVID-19 pandemic has created an unprecedented global economic downturn that includes record-breaking unemployment, declining consumer confidence, and potential financial calamity that marvels the Great Depression. The sharp global contraction of economic activity resulting from COVID-19 is changing how organizations operate. Organizations are cutting expenses, working remotely, and laying off or furloughing employees — all of which weaken employee morale. Because businesses are ultimately driven by the actions of their employees, the combination of these adverse conditions on employees' psyche has increased the vulnerability and heightened the risk for corporate fraud.

> Following the 2008-09 financial crisis, 84% of companies cited some level of fraud occurrence. Are organizations prepared this time around?

Fraud is a problem affecting organizations worldwide. According to the Association of Certified Fraud Examiners (ACFE), the world's largest anti-fraud association, organizations lose approximately 5% of their revenue to fraud each year.[1] With a projected $90 trillion world economy, that translates to more than $4.5 trillion in annual global fraud losses.[2] Despite the financial and reputational implications stemming from fraud losses, fraud risk may not be considered a top priority by management during an economic downturn as organizations deal with financial, operational, and other competing priorities to keep their businesses afloat. Management may also rationalize that during a time of crisis, its employees would not resort to fraud and take a "that would never happen here" mentality.

While most organizations predominately consist of ethical employees who abide by established Codes of Conduct, the unfortunate reality is that the COVID-19 pandemic is creating an environment ripe for fraudulent activity, as seen during past economic crises.

During this current crisis, the pressure on management to deliver financial results is exacerbated, it creates unprecedented opportunities for wrongdoers due to disruption within organizations, and employees' moral compasses are pushed to the limit as people may enter a self-preservation mode. In a March 2020 press

1 *2020 Report to the Nations*. Copyright 2020 by the Association of Certified Fraud Examiners, Inc.
2 *International Monetary Fund*, World Economic Outlook Database, October 2019.
https://www.imf.org/external/pubs/ft/weo/2019/02/weodata/index.aspx

release, the ACFE's president and CEO indicated "… the looming economic downturn we can expect to see has a number of long-lasting implications. One important one being an explosion of fraud in the coming years — and organizations need to brace themselves."[3]

Within this article, I lay out a blueprint of how management can navigate corporate fraud within its organization. As organizations adapt to the new normal caused by the COVID-19 pandemic, this blueprint includes:

- Assessing where they are most vulnerable to fraud
- Instituting fraud mitigation procedures to protect the organization
- Actively monitoring for fraud red flags

3 "Coronavirus Pandemic Is a Perfect Storm for Fraud," Association of Certified Fraud Examiners, Inc., March 31, 2020. https://www.acfe.com/press-release.aspx?id=4295010491. Press release.

HISTORICAL PARALLEL

The most recent economic downturn with the breadth and scale our economy is currently experiencing was during the 2008-09 global financial crisis. While many comparisons are being drawn between the two calamities, organizations should reflect on the lessons learned during the last crisis so mistakes are not repeated. Gaining an understanding of the interrelationship between fraud and an economic downturn is an important exercise.

Following the 2008-09 global financial crisis, the ACFE conducted a survey of hundreds of anti-fraud professionals to assess the impact and correlation between the economic downturn and the instances of fraud.[4] Highlights of the fraud survey included:

- During the financial crisis, 55% of respondents observed an increased level of fraudulent activity and 29% observed the same level of fraud occurrence since the beginning of the financial crisis.
- 88% of respondents anticipated an increase in the level of fraudulent activity.
- Less than 2% of respondents believed that there would be lower instances of fraud during times of economic distress.

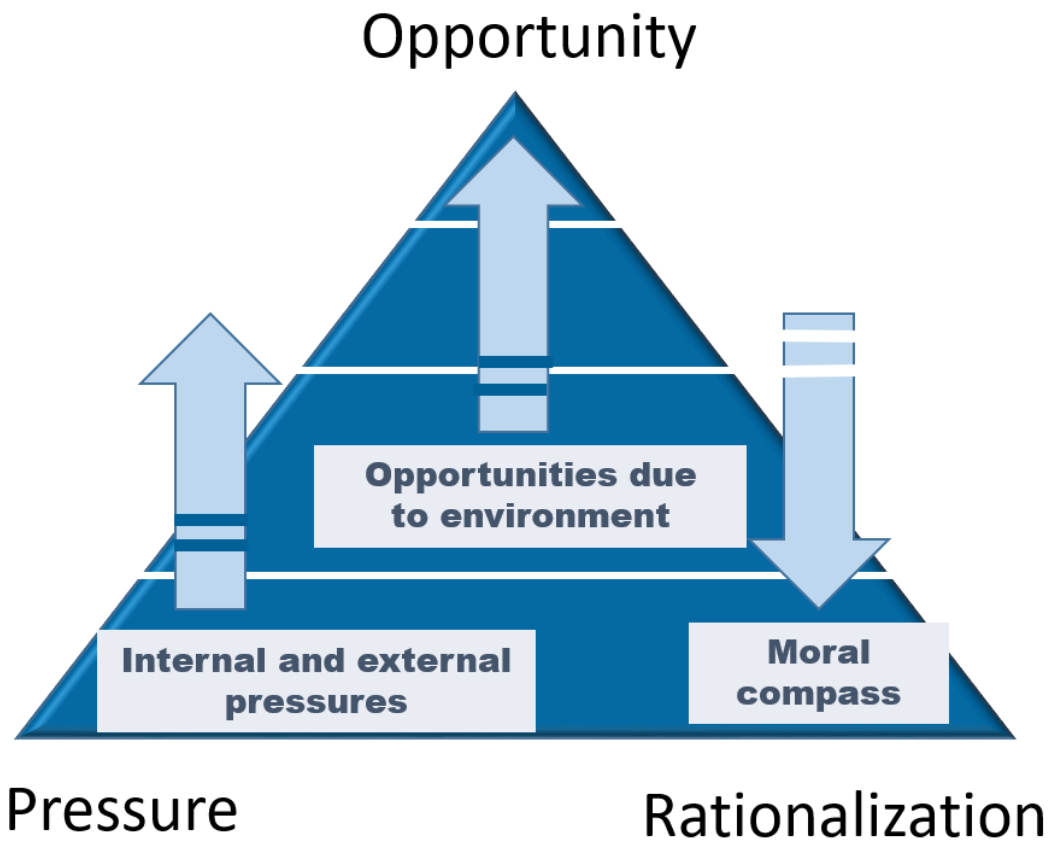
A Perfect Fraud Storm Is Brewing

As organizations assess where they are most vulnerable to fraud, getting inside the heads of their employees to understand what motivates wrongdoing will enable management to focus on mission-critical mitigation procedures and internal controls necessary to weather the brewing fraud storm. The well-known fraud deterrence and detection framework model known as the fraud triangle (developed in the 1950s by criminologist Donald Cressey) remains a widely accepted predictive model that explains why people commit fraud. The fraud triangle provides the drivers that allow a fraudulent event to occur and relies on the interrelationship between the following three elements: pressure, opportunity, and rationalization (see figure 1). For fraud to occur, typically all three elements are present.

1. Pressure refers to an employee's motivation and mindset toward committing fraud.
2. Opportunity refers to circumstances that allow fraud to occur and is the only component over which an organization exercises some level of control.
3. Rationalization refers to an individual's justification for committing fraud.

4 *Occupational Fraud: A Study of the Impact of an Economic Recession*. Copyright 2009 by the Association of Certified Fraud Examiners, Inc.

Figure 1: The Fraud Triangle



The premise is that to combat fraud, organizations (including its internal auditors) should assess how the COVID-19 pandemic affects employee sentiment and may impact these three elements. One of the reasons for the heightened risk for corporate fraud during an economic downturn is that all three elements of the fraud triangle are negatively impacted.

The Institute of Internal Auditors (IIA) President and CEO Richard Chambers describes the current economic downturn as one where occupational fraud can thrive. He cautions, "Anyone with the slightest understanding of fraud is familiar with the concept of the fraud triangle, which identifies pressure, opportunity, and rationalization as the key ingredients. The pandemic is fueling the first — pressure — in myriad ways, as its impact on economies threatens the financial well-being of millions of organizations and billions of workers globally."[5] Organizations should assess their current situations and figure out which elemental drivers are being impacted. Having knowledge to identify those indicators of fraud will enable them to support their organizations to improve the performance of their fraud controls and risk management processes.

5 Richard Chambers, "Fraud Report Affirms Internal Audit's Value at Critical Time," *Internal Auditor*, April 27, 2020. https://iaonline.theiia.org/blogs/chambers/2020/Pages/Fraud-Report-Affirms-Internal-Audits-Value-at-Critical-Time.aspx

Table 1 lists examples of internal and external drivers that may impact employee behavior during the COVID-19 pandemic.

Table 1: Examples of Internal and External Drivers Impacting Employee Behavior

DRIVERS	INTERNAL AND EXTERNAL EXAMPLES
Pressure	• **Motivation:** Employees may feel financial, emotional, and/or mental instability pressures. • **Analyst expectations:** Meet financial targets of the organization. • **Financial difficulties:** As corporate profits decrease, executives may be pressured, especially when their compensation is linked to the financial performance of the organization (e.g., sales personnel attempting to meet their sales targets). • **Incentive compensation:** With salary reductions and the elimination of bonuses and other forms of compensation, employees may want to find ways to replace lost wages to maintain their standard of living. • **Layoffs:** While well-intentioned, management may feel pressured to paint a rosier picture of its financial position to limit workforce layoff plans. • **Job insecurity:** During times of grave uncertainty, employees' loyalty may come into question and some may be more willing to bend certain accounting rules to remain in good favor with management as a form of self-preservation. • **Medical bills:** There is the potential of mounting medical bills for employees and their family members who have been affected by the virus.
Opportunity	• **Limited management oversight:** Employees are working remotely with limited to no management oversight, which makes it easier to override and circumvent controls. • **Impact on internal controls:** Organizations are downsizing and eliminating positions, which has an immediate effect on a potential lack of segregation of duties. Critical internal controls may be overlooked. • **Competing priorities:** Organizations are focusing on operational and financial priorities, and fraud risk mitigation may not be a top priority right now. • **Reduced budgets:** Organizations are decreasing budgets and having to do more with less. • **Neglecting international operations:** Organizations may be focusing on domestic operations and neglecting their international operations that may pose the highest levels of bribery and corruption risk. Organizations may be failing to complete their planned audits at high-risk locations.
Rationalization	• **Moral compass:** Employees' moral compass may be impacted as they become anxious during the COVID-19 pandemic. • **Psyche:** Employees' psyche may perceive improper behavior differently during times of crisis and may justify such behavior. • **Loyalty:** Employees' loyalty may decrease as they enter a mode of self-preservation. • **Perception:** Employees may think their organization is focusing on larger issues rather than nonmaterial fraud. • **Justification:** "The company owes me!" • **Justification:** "We are in a time of crisis and I need to support my family at all costs."

THREE LINES MODEL: FRAUD MITIGATION CONCERNS

After assessing employee sentiment, organizations will need to adapt their risk management and control frameworks to focus on fraud mitigation. Organizations using the traditional three lines risk management model to manage their risks will need to revisit their continuity plans on how to effectively enhance communications on risk management/controls and management's roles and responsibilities. The three lines model can enhance the effectiveness of risk management systems by properly coordinating with the different stakeholders within and outside the organization.

1. **First line.** Operational management are the process owners and their function is to own and manage the organization's risks.
2. **Second line.** Risk and compliance management function oversees or specializes in compliance or the management of risk.
3. **Third line.** Internal audit serves to provide independence and objectivity on the effectiveness of risk management functions.

During the COVID-19 pandemic, the three lines stakeholder group needs to remain vigilant to ensure proper fraud mitigation procedures are in place. Based on an April 2020 poll by The IIA's Audit Executive Center, 40% of respondents indicated that their internal audit functions have added focus on cybersecurity, enterprise risk management, fraud, and cost control/reduction.[6]

The organization should take a fresh look at the areas within the business most vulnerable as a result of this crisis. This will allow management the opportunity to identify any significant gaps and modify or implement controls with proper management oversight to reduce the likelihood and impact of those fraud risks. Identified gaps and susceptible controls need to be revisited and updated in order to prevent and detect the increased fraud risks. Management should recognize that due to changing market conditions, controls need to be updated to reflect the current environment and aligned to its risk management strategy. During the COVID-19 pandemic, it is easy for an organization to be distracted and lack the discipline necessary to address its highest fraud risks.

As organizations attempt to remain vigilant, table 2 provides several fraud mitigation procedures that each three lines stakeholder should consider throughout the COVID-19 pandemic, which is now expected to last significantly longer and affect every country.

6 *COVID-19 Impact on Internal Audit.* Copyright 2020 The Institute of Internal Auditors, Inc.

Table 2: Fraud Mitigation Procedures for Three Lines Stakeholders

FIRST LINE: OPERATIONAL MANAGEMENT	SECOND LINE: FINANCIAL CONTROLLER, RISK MANAGEMENT, COMPLIANCE	THIRD LINE: INTERNAL AUDIT
✓ Tone at the top — senior management needs to be visible in its commitment to combatting corporate fraud. ✓ Prioritize areas of fraud risk that pose the highest levels of financial, regulatory, and reputational risk. ✓ Institute a new or reinforce an existing zero tolerance policy against fraud and corruption. ✓ Review remediation plans of previous fraud incidents for lessons learned (e.g., vulnerable areas exploited following the 2008-09 financial crisis). ✓ Become more involved in performing management reviews of accounting estimates. ✓ Review corporate insurance policy coverages to ensure that the organization is protected from fraud risks.	✓ Promote and adequately reinforce communication regarding the whistleblower hotline. ✓ Create an environment where employees are motivated to report wrongdoing.[A] ✓ Conduct targeted fraud training for employees, especially for managers in high-risk areas of the business. ✓ With increasing levels of layoffs and furloughs, assess whether there is proper coverage to mitigate the fraud risks. ✓ Based on existing technology, determine what types of automated analytics could be leveraged to mitigate fraud risks. ✓ Expand audit procedures to help mitigate fraud risks. ✓ Evaluate the appropriateness of accounting policies used. ✓ Review the reasonableness of significant accounting estimates that have varying degrees of management judgment, especially in accounts significantly impacted by the COVID-19 pandemic.[B]	✓ Reassess modified fraud controls that account for changing circumstances, such as controls that were suspended. ✓ Advise on the strengthening of vulnerabilities within the IT infrastructure focusing on information security assessments. ✓ Update continuous monitoring auditing tools to reflect the post-COVID-19 world. ✓ Perform proactive forensic data analytics to identify high-risk transactions. ✓ Perform surprise audits. ✓ Revisit prior fraud risk assessments and pressure test fraud schemes deemed as highest risk (high significance, high likelihood).

[A] Surveys indicate that tips are the number one detection method for uncovering fraud. Accordingly, with reduced workforces and attention focused on other priorities, organizations need as many eyes and ears as possible to report potential wrongdoing. An organization should promote awareness of the importance of its corporate compliance program, remind its employees of the hotline, and provide clear instructions on how to report a tip. Organizations should stress that they take their whistleblower reports seriously, reports are maintained confidential, procedures are in place to maintain whistleblower anonymity, and there should be no fear of retaliation. Reporting mechanisms should be made available to all groups within the organization both domestically and internationally, in local languages, and to third parties outside the organization, such as customers and suppliers.

[B] Internal auditors should consider that U.S. Generally Accepted Accounting Principles (GAAP) is not one size fits all. GAAP is comprised of a series of rules and standards for financial reporting. GAAP is based on certain fundamental objectives and key concepts required of financial statements to be useful to various stakeholders and other users of the financial statements. Throughout this collection of rules and standards, the organization's management is required to make various judgments regarding the business based on its history and knowledge of the ongoing operations. It is widely accepted that, "[t]o a large extent, financial reports are based on estimates, judgments, and models rather than exact depictions" (FASB Conceptual Framework 8, OB11). GAAP allows for certain management discretion in the application of various policies, estimates, methodologies, and analysis to arrive at the required balance of assets and liabilities. This discretion could allow management to push the envelope in its estimates, and the reasonableness of its accounting estimates should be scrutinized.

RECOGNIZING THE FRAUD RED FLAGS

Once the three lines stakeholder group has successfully adapted its risk management framework with fraud mitigation procedures, it needs to actively monitor for red flags associated with the fraud schemes being perpetrated against its organization. The first step is for management to recognize what type of employees traditionally fit the typical fraudster profile. According to the ACFE and other leading fraud surveys, the most common risk profile of a fraudster includes:

- More likely to be a male between the ages of 36 and 45
- May work within one of the following departments that are most susceptible to fraud: operations, accounting, executive management, sales
- Has a university degree or higher
- Most fraud cases are perpetrated by those with a tenure of < 5 years, but the highest median fraud losses are caused by those with a tenure of 6+ years

The second step is for the organization to actively monitor for fraud schemes with high likelihood of occurrence due to the COVID-19 pandemic. As described earlier, the opportunity for an employee to commit wrongdoing is easier in this environment. When employees work remotely, there may be a lack of management oversight, making it easier to override controls. While the risk profile for each organization may be different, fraud schemes can be categorized into three primary occupational fraud areas: corruption, asset misappropriation, and financial statement fraud. The most damaging fraud schemes in terms of losses are typically within the financial statement fraud area. An article published in *The Economist* claims the COVID-19 pandemic will likely give rise to new fraud schemes, hinting that when "economic survival is threatened, the line separating what is acceptable and unacceptable when booking revenue or making market disclosures can be blurred."[7] Nevertheless, as each organization is unique, it will need to assess its own risks. For instance, organizations accepting funding from the federal government in connection with the CARES Act should consider whether there is any abuse of the received government funds. Organizations are also particularly vulnerable to cyber threats during the crisis and may need to take extra precautions to protect any intellectual property that is paramount to their operations.

7 "Who's lost their trunks? The economic crisis will expose a decade's worth of corporate fraud," *The Economist*, April 18, 2020. https://www.economist.com/business/2020/04/18/the-economic-crisis-will-expose-a-decades-worth-of-corporate-fraud

While each organization is unique based on its risk profile (e.g., industry, geography), table 3 lists a broad range of red flags of what companies may be vulnerable to during the COVID-19 pandemic.

Table 3: Examples of Fraud Red Flags During a Pandemic

CORRUPTION	ASSET MISAPPROPRIATION	FINANCIAL STATEMENT FRAUD
✓ Questionable use of third-party agents, consultants, or sales intermediaries who interact with government officials ✓ Insider trading ✓ Bribing to obtain or retain new business (or funding from government programs)	✓ Larceny of inventory ✓ Frequency of purchases and amount of vendor spend sharply increasing ✓ Volume of purchases not supported by a rational need ✓ Lack of physical control over assets ✓ Overstating or creating fictitious expenditures ✓ Falsifying hours leading to overstatement of compensation	✓ Sales exactly meet budget or expectations ✓ Bonuses tied to sales ✓ Excessive returns after period-end ✓ Customer invoices show extended payment terms or unusual return allowances ✓ Improper inventory and other asset valuations ✓ Unapproved changes to vendor master file are unauthorized ✓ Pressure to manipulate financial estimates ✓ Write-downs to cover account shortfalls ✓ Data manipulation to breach financial covenants

Cyber Threats Risk Mitigation – An Absolute Must

In addition to the occupational fraud risks described above, cybercrime poses a unique set of challenges. As the COVID-19 pandemic sweeps the world and millions have shifted to working remotely, the risk of being victimized by a cyber threat (such as phishing attacks and business email compromises) has substantially increased. Cybercriminals are already moving at accelerated paces to take advantage. Within the first six weeks following the announcement of the first COVID-19 case reported in the U.S., the Federal Bureau of Investigation (FBI) developed a dedicated site on its official webpage urging vigilance during the COVID-19 pandemic.[8] The FBI issued several fraud warnings to the public linked to the COVID-19 pandemic dealing with cyber threats, business email compromise schemes, emerging health-care fraud schemes, and cryptocurrency scams, among others.

Organizations need to remain vigilant during the new paradigm shift of moving their workforce remotely to prevent phishing attacks and remind their employees of this risk. As organizations review their policies and procedures to mitigate a cyberattack, three lines stakeholders should actively communicate across differing departments within the organization. Mitigating cyber threats should be an enterprisewide effort and not one solely focused on IT departments. Organizations should implement additional preventative measures to protect their crown jewels.

8 "FBI Urges Vigilance During COVID-19 Pandemic," Federal Bureau of Investigation. https://www.fbi.gov/coronavirus

Organizations can send brief “Did you know” type emails to their employees with best practice ideas, including:

- Remain alert against cyber threats that can originate from manipulated emails, URLs, text messages, and phone calls.
- Be cautious when clicking on unfamiliar links.
- Think twice before providing corporate financial data and personal information.
- Be cautious of downloading a file without verifying it.

Global Risks

As organizations assess their risk profiles, it is imperative that they consider the international business risks related to fraud, bribery, and corruption. Organizations operating in high-risk markets need to assess their local market knowledge and the potential ramifications of disregarding fraud risks. The three lines stakeholder group should ensure that its fraud-fighting team is focusing its efforts on the highest probable fraud risks in the right emerging market locations. If organizations are scaling back and cancelling certain planned audits in high-risk markets, they should consider challenging whether that makes sense given the risk exposure.

One example of a global risk barometer that organizations could turn to is Transparency International’s (TI’s) Corruption Perceptions Index (CPI). TI is a nonprofit organization with national chapters in more than 100 countries. Its mission is to combat global corruption, promote transparency, and prevent criminal activities arising from corruption. The CPI generally defines corruption as the misuse of public power for private benefit and ranks 180 countries and territories by their perceived levels of public sector corruption from 100 (very clean) to zero (highly corrupt). Countries ranked below 40 are deemed to have serious corruption problems. For instance, management of U.S. multinationals operating in low-ranked CPI countries need to factor in the heightened level of regulatory risk due to higher likelihood of corruption.

SUMMATION

As the COVID-19 pandemic continues to wreak havoc on global markets, the perfect fraud storm is brewing. Organizations are more vulnerable to corporate fraud as all three elemental drivers impacting employee behavior (pressure, opportunity, and rationalization) are negatively heightened. This crisis is creating unprecedented disruption and opportunities for corporate wrongdoers. Anti-fraud specialists and past crises signal that a significant uptick of fraud is just around the corner.

Management needs to act swiftly to adapt its risk management and control frameworks to ensure proper fraud mitigation procedures are in place. The earlier action is taken, such as promoting its whistleblower hotline, the higher the likelihood that an organization can mitigate expensive investigation costs and legal and regulatory infractions. Management should understand it's most common fraud risks and prioritize the areas that pose the highest levels of financial, regulatory, and reputational risks. This will enable organizations to actively monitor for red flags associated with fraud schemes with high likelihood of occurrence due to the COVID-19 pandemic, with an emphasis on combating cyber threats.

Fraud is an unfortunate fact of life and is impacted by internal and external factors. As organizations adapt to the economic downturn and new working conditions due to the COVID-19 pandemic, they need to adapt and work creatively to protect against fraud that is related to financial losses, enforcement penalties, and loss of reputation. Is your organization assessing employee sentiment and properly prepared to navigate the brewing fraud storm?

About the Internal Audit Foundation

The Internal Audit Foundation strives to be an essential global resource for advancing the internal audit profession. The Foundation's research and educational products provide insight on emerging topics to internal audit practitioners and their stakeholders and promotes and advances the value of the internal audit profession globally. Through the Academic Fund, the Foundation supports the future of the profession by providing grants to students and educators who participate in The IIA's Internal Auditing Education Partnership Program. For more information, visit www.theiia.org/Foundation.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is located in Lake Mary, FL. For more information, visit www.theiia.org.

About FLAI

Fundación Latinoamericana de Auditores Internos (FLAI) is a professional, nonprofit, independent organization. Its mission is to promote and support the continuous development of the internal audit profession in Latin America, fostering regional cooperation and integration. Established in 1995, it is an organization associated with The Institute of Internal Auditors (IIA) and represents 16 regional Institutes of Internal Auditors with more than 13,500 members. For more information, visit www.laflai.org.

Disclaimer

Copyright

The Institute of Internal Auditors

INTERNAL AUDIT FOUNDATION™

FLAI
FUNDACIÓN LATINOAMERICANA DE AUDITORES INTERNOS