جهاز أبوظبي للمحاسبة
ABU DHABI ACCOUNTABILITY AUTHORITY

NAZAHA

A periodical dedicated to raise awareness about the risks of violations and fraud, issued by the Integrity & Accountability Unit at the Abu Dhabi Accountability Authority

Volume 2 - 2019

معاً نحمي المال العام
Together Safeguarding Public Funds
www.adaa.abudhabi.ae

Together, Safeguarding Public Funds

The European Commission adopted on April 29, 2019 a new Anti-Fraud Strategy that seeks to further improve the detection, sanctioning and prevention of fraud and will support the Commission's ongoing efforts to bring fraud against the European Union budget further down. The new Strategy pushes for more consistency and better coordination in the fight against fraud among the various Commission departments and paves the way for more data-driven anti-fraud measures in the coming years. The vision behind the new Strategy is to strengthen the corporate oversight of the Commission regarding all issues related to fraud and to reinforce the anti-fraud system that is already in place. Günther H. Oettinger, European Commissioner for Budget and Human Resources, stated on this occasion that: "The European Commission has zero tolerance to fraud. Every euro from the EU budget should be well spent and should create added value for the EU citizens. Today's Strategy will help us stay focused on preventing, detecting and stopping fraud. We must always remain one step ahead of fraudsters."

Building on actions taken since 2011, the new Strategy seeks to make sure that the Commission makes the most out of the available data to prevent and detect fraud. It focuses on improving the quality and completeness of relevant information, on joining up different data sources and on creating smarter tools to draw operational conclusions. The Strategy also seeks to reinforce the Commission's corporate oversight of fraud issues, by giving the European Anti-Fraud Office (OLAF) a much stronger advisory and supervisory role. OLAF will conduct mandatory reviews of the anti-fraud strategies of all Commission Directorates and monitor their implementation. It will liaise with all departments, and especially with the Heads of the Commission's central services (Secretariat-General, Legal Service, DG Human Resources and DG Budget), in this process. This will strengthen the Commission's overall governance of the anti-fraud system. In addition, the Commission will strengthen its follow-up of OLAF´s recommendations in order to ensure a better implementation.

The Commission initially adopted its "Commission Anti-Fraud Strategy" (CAFS) in 2011. It set out at the time guidelines for the Commission's fight against fraud, such as the principle of zero tolerance to fraud, and three priority actions, namely: (i) introducing anti-fraud provisions in Commission proposals on spending programmes under the Multi Annual Financial Framework for 2014-2020; (ii) implementing anti-fraud strategies at department level; and (iii) revising the public procurement directives. The general guidelines remain valid and the measures provided for in the 2011 CAFS have been fully implemented.

> **"Building good citizens is more difficult than building factories. Sophisticated nations are judged by the level of their population's education"**
>
> The Late Sheikh
> Zayed Bin Sultan Al Nahyan

The Commission services consequently performed an evaluation of the 2011 CAFS. The evaluation concluded that although the CAFS is still relevant and effective as a policy framework for the Commission in protecting the EU budget, it needs to adapt to an evolving situation (new funding schemes and fraud trends, development of IT tools, etc.). For the review of the CAFS, the Commission carried out a fraud risk assessment, involving the executive agencies. Thus, the 2019 CAFS also addressed some key recommendations issued by the European Court of Auditors in a Special Report entitled "Fighting fraud in EU spending: action needed", and complemented the Commission's 'Governance Package', adopted in November 2018, which designates OLAF as the lead service in the conception and development of a European anti-fraud policy and further assigns a strategic role regarding corporate aspects of the fight against fraud to the Corporate Management Board. The Corporate Management Board brings together the Commission's Secretary-General and the Directors-General of its central services (budget, human resources and legal affairs).

Introductory view: The Bribery Act 2010

The UK Bribery Act 2010 (The Act) is concerned with bribery. Very generally, this is defined as giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly or to reward that person for having already done so. So this could cover seeking to influence a decision-maker by giving some kind of extra benefit to that decision maker rather than by what can legitimately be offered as part of a tender process. The Act thus deals exclusively with bribery, and does not address other white collar crimes and is not concerned with fraud, theft, books and record offences, Companies Act offences, money laundering offences or competition law. An organisation could be liable if a very senior person in this organisation (for example, a managing director) commits a bribery offence. This person's activities would then be attributed to the organisation as a whole. An organisation could also be liable where someone who performs services for it - like an employee or agent - pays a bribe specifically to get business, keep business, or gain a business advantage for that organisation, who may still have a full defence for this particular offence, and can avoid prosecution, if it can demonstrate that it had implemented adequate procedures in place to prevent bribery.

The UK Government, upon issuing this legislation, considered that procedures put in place by commercial organisations wishing to prevent bribery being committed on their behalf should be informed by the following six principles: "Proportionate Procedures", "Top-Level Commitment", "Risk Assessment", "Due Diligence", "Communication (including training)", and "Monitoring and Review". These principles are not prescriptive, but are rather intended to be flexible and outcome focussed, allowing for the huge variety of circumstances that commercial organisations find themselves in. Small organisations will, for example, face different challenges to those faced by large multi-national enterprises. Accordingly, the detail of how organisations might apply these principles, taken as a whole, will vary, but the outcome should always be robust and effective anti-bribery procedures. In short, bribery prevention procedures should be proportionate to risk. Although commercial organisations with entirely

domestic operations may require bribery prevention procedures, the general proposition is that they will face lower risks of bribery on their behalf by associated persons than the risks that operate in foreign markets. In any event procedures put in place to mitigate domestic bribery risks are likely to be similar if not the same as those designed to mitigate those associated with foreign markets. The principles will be elaborated on in this and future editions.

Principle 1:
Proportionate procedures

A commercial organisation's procedures to prevent bribery by persons associated with it are proportionate to the bribery risks it faces and to the nature, scale and complexity of the commercial organisation's activities. They are also clear, practical, accessible, effectively implemented and enforced.

> Commentary

- The term 'procedures' is used in this text to embrace both bribery prevention policies and the procedures which implement them. Policies articulate a commercial organisation's anti-bribery stance, show how it will be maintained and help to create an anti-bribery culture. They are therefore a necessary measure in the prevention of bribery, but they will not achieve that objective unless they are properly implemented.

- Adequate bribery prevention procedures ought to be proportionate to the bribery risks that the organisation faces. An initial assessment of risk across the organisation is therefore a necessary first step. To a certain extent, the level of risk will be linked to the size of the organisation and the nature and complexity of its business, but size will not be the only determining factor. Some small organisations can face quite significant risks, and will need more extensive procedures than their counterparts facing limited risks. However, small organisations are unlikely to need procedures that are as extensive as those of a large multi-national organisation. For example, a very small business may be able to rely heavily on periodic oral briefings to communicate its policies while a large one may need to rely on extensive written communication.

- The level of risk that organisations face will also vary with the type and nature of the persons associated with it. For example, a commercial organisation that properly assesses that there is no risk of bribery on the part of one of its associated persons will accordingly require nothing in the way of procedures to prevent bribery in the context of that relationship. By the same token the bribery risks associated with reliance on a third party agent representing a commercial organisation in negotiations with foreign public officials may be assessed as significant and accordingly require much more in the way of procedures to mitigate those risks. Organisations are likely to need to select procedures to cover a broad range of risks but any consideration by a court in an individual case of the adequacy of procedures is likely necessarily to focus on those procedures designed to prevent bribery on the part of the associated person committing the offence in question.

- Bribery prevention procedures may be stand alone or form part of wider guidance, for example on recruitment or on managing a tender process in public procurement. Whatever the chosen model, the procedures should seek to ensure there is a practical and realistic means of achieving the organisation's stated anti-bribery policy objectives across all of the organisation's functions.

- The UK Government recognises that applying these procedures retrospectively to existing associated persons is more difficult, but this should be done over time, adopting a risk-based approach and with due allowance for what is practicable and the level of control over existing arrangements.

> Procedures

- Commercial organisations' bribery prevention policies are likely to include certain common elements. As an indicative and not exhaustive list, an organisation may wish to cover in its policies:

  • Its commitment to bribery prevention.

  • Its general approach to mitigation of specific bribery risks, such as those arising from the conduct of intermediaries and agents, or those associated with hospitality and promotional expenditure, facilitation payments or political and charitable donations or contributions; an overview of its strategy to implement its bribery prevention policies.

- The procedures put in place to implement an organisation's bribery prevention policies should be designed to mitigate identified risks as well as to prevent deliberate unethical conduct on the part of associated persons. The following is an indicative and not exhaustive list of the topics that bribery prevention procedures might embrace depending on the particular risks faced:

- The involvement of the organisation's top-level management.

- Risk assessment procedures.

- Due diligence of existing or prospective associated persons.

- The provision of gifts, hospitality and promotional expenditure; charitable and political donations; or demands for facilitation payments.

- Direct and indirect employment, including recruitment, terms and conditions, disciplinary action and remuneration.

- Governance of business relationships with all other associated persons including pre and post contractual agreements.

- Financial and commercial controls such as adequate bookkeeping, auditing and approval of expenditure.

- Transparency of transactions and disclosure of information.

- Decision making, such as delegation of authority procedures, separation of functions and the avoidance of conflicts of interest.

- Enforcement, detailing discipline processes and sanctions for breaches of the organisation's anti-bribery rules.

- The reporting of bribery including 'speak up' or 'whistle blowing' procedures.

- The detail of the process by which the organisation plans to implement its bribery prevention procedures, for example, how its policy will be applied to individual projects and to different parts of the organisation.

- The communication of the organisation's policies and procedures, and training in their application.

- The monitoring, review and evaluation of bribery prevention procedures.

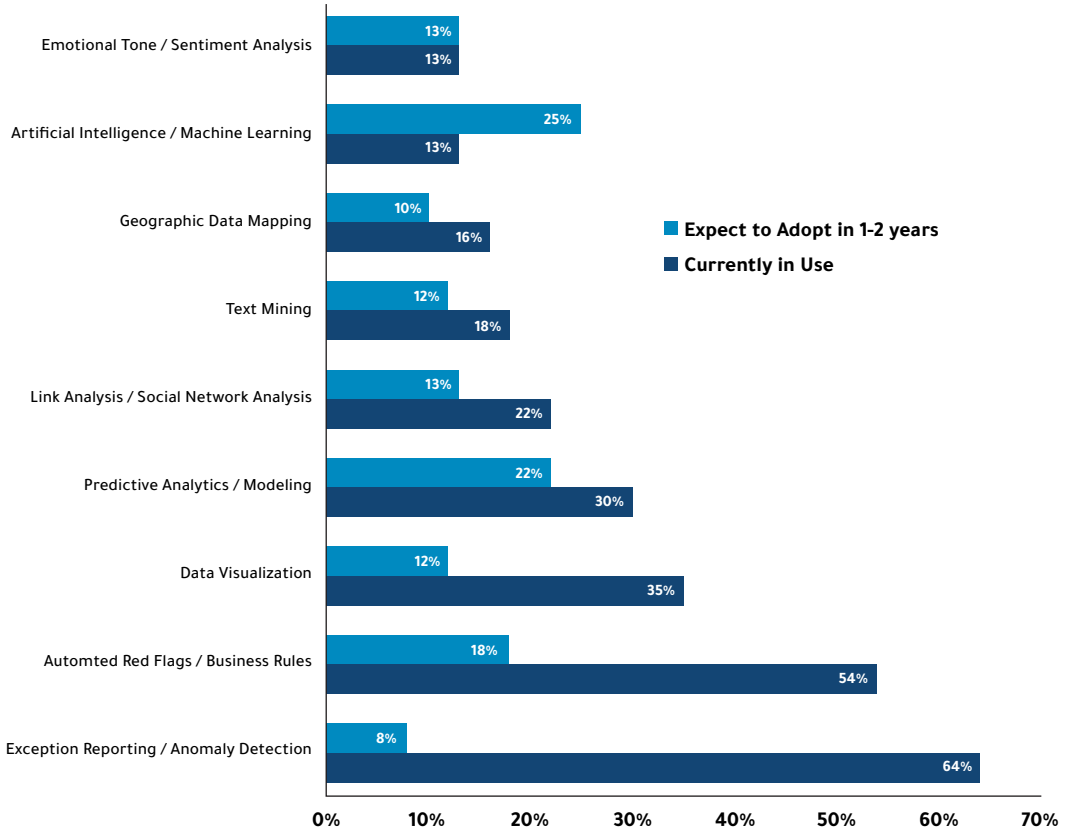
Did you know

The first edition of the "Anti-Fraud Technology Benchmarking Report" has just been released by The Association of Certified Fraud Examiners (ACFE), in partnership with "SAS". The report presents the results of a benchmarking study to help organizations understand what anti-fraud technologies their peers are using and to assist in guiding future adoption of such technologies to further assist those organizations to effectively evaluate them so that they can remain one step ahead of potential fraud perpetrators.

Technological advancements present opportunities for both fraud perpetrators and those trying to stop them. As criminals find new ways to exploit technology to commit their schemes and target new potential victims, anti-fraud professionals must ensure they are likewise adopting new technologies that are the most effective in navigating the evolving threat landscape.

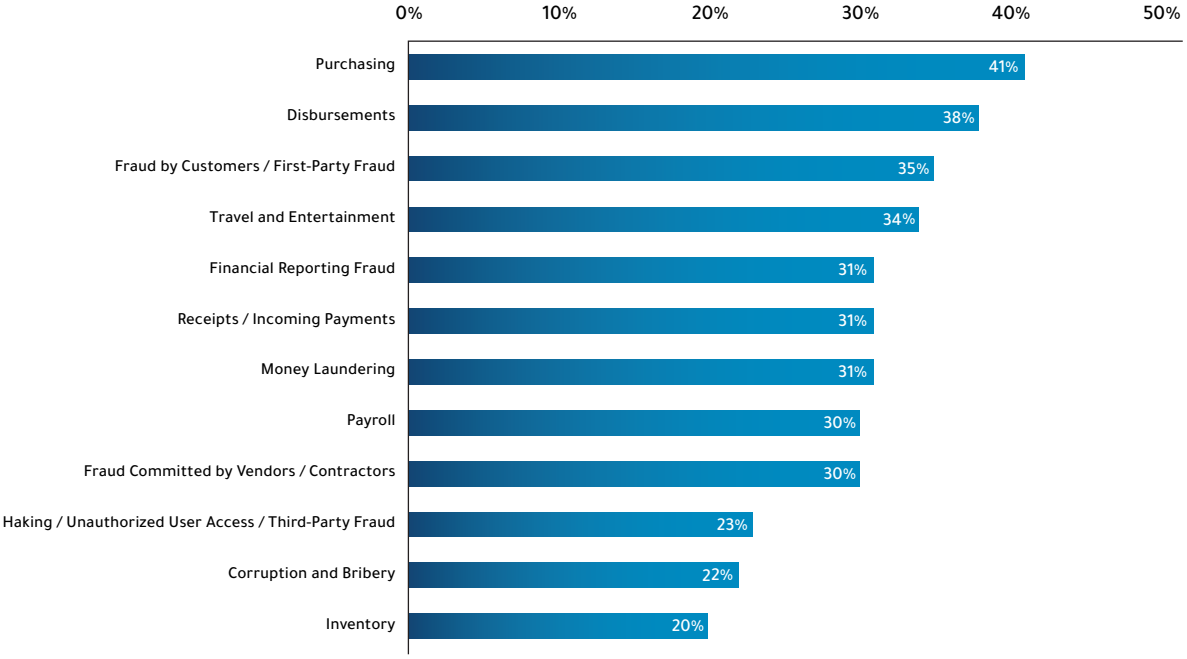
The approach followed was to send a 19-question survey to 41,181 randomly selected ACFE members, where respondents were asked to provide information about their organizations' use of various technologies as part of their anti-fraud initiatives. Survey responses were collected anonymously, and a total of 2,255 survey responses were received out of which 1,055 were usable for purposes of this benchmark.

The results as collated provided relevant insights on how the profession, and professionals, are approaching this domain, as explained in the captions that follow:



> With regard to fighting fraud, a variety of techniques and technologies can be used to analyze data in order to find red flags and control gaps that might indicate the potential for misconduct. Survey respondents were thus asked about the types of data analytics their organizations currently use as part of their anti-fraud initiatives, as well as the types of analytics they expect their organizations to adopt or deploy in the next one to two years. The figure that follows shows that nearly two-thirds of organizations currently use exception reporting or anomaly detection techniques in their fraud-related initiatives, and more than half have implemented automated monitoring of red flags or violations of business rules. These types of techniques are often considered among the more traditional analytic approaches and have been used in the anti-fraud field the longest of the techniques, so it stands to reason that they have been adopted by the largest percentage of organizations. The survey data also indicates that these analytic approaches will continue to be the most common, with a total of 72% of organizations expecting to use each of these techniques over the next two years. Data visualization and predictive analytics/ predictive modeling are comparatively newer types of analytics techniques that have been or are expected to be adopted by a significant portion of organizations. In the next two years, these types of analytics are likely to be used by a cumulative 47% and 52% of organizations, respectively, as part of their anti-fraud initiatives:

> The decision to use data analytics to monitor for fraud within specific business functions and operations often varies based on numerous factors, including access to data, technological or process limitations, and assessed level of risk. Respondents were asked to note the risk areas for which their organizations currently use data analytics or automated monitoring tools to identify red flags of potential fraud. In general, organizations are proactively monitoring their data across numerous fraud risk areas, with the most prominent being purchasing (41%), disbursements (38%), fraud by customers/first-party fraud (35%), and travel and entertainment (34%), as presented in the figure that follows.



> When attempting to implement new anti-fraud technologies, obtaining management buy-in can be a challenge for many organizations. Part of overcoming this challenge involves being able to articulate and prove the benefits that such technology can provide. The survey respondents who are currently employing data analytics in their anti-fraud programs, were asked how beneficial the use of this technology has been with regard to the following considerations:

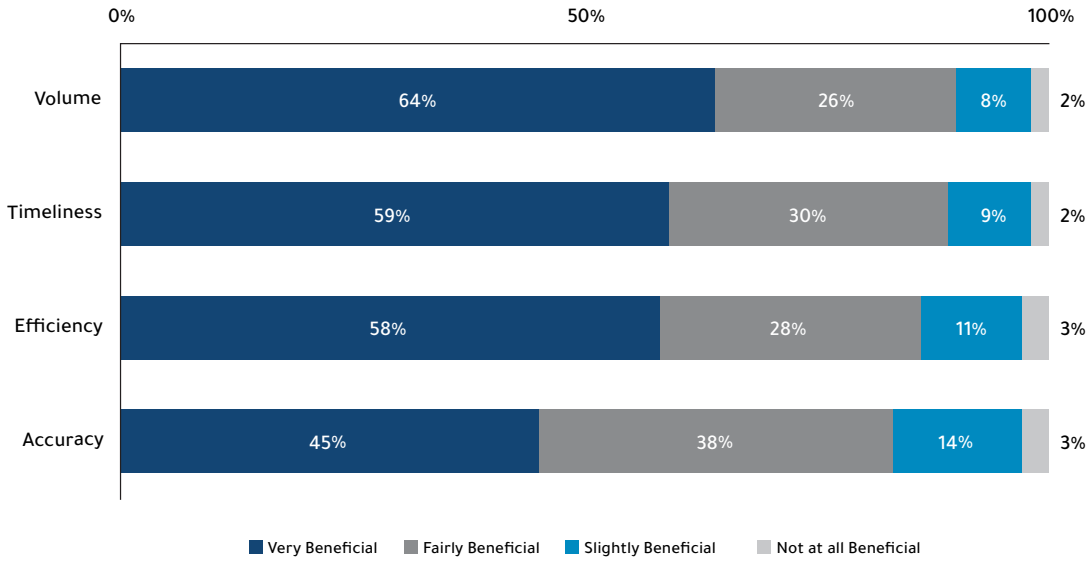
- Volume, enabling them to review more transactions and identify more cases of suspected fraud

- Timeliness, allowing them to detect anomalies more quickly

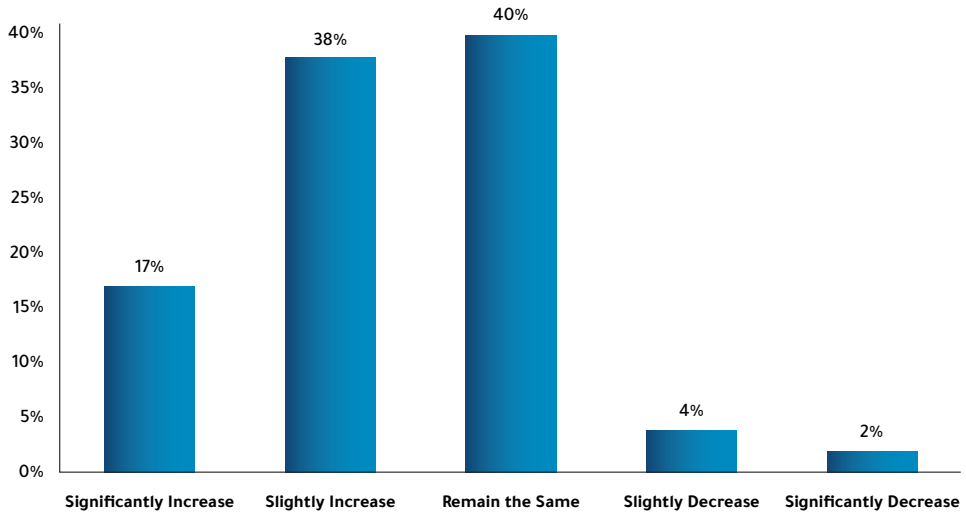
- Efficiency, by automating time-consuming tasks

- Accuracy, resulting in a reduced false-positive rate

The figure that follows shows that the vast majority of organizations experience substantial benefits from their use of anti-fraud analytics, with 83% to 90% of organizations rating their analytics programs as being either very beneficial or fairly beneficial in each of these four areas. The top benefit realized pertains to volume: 64% of survey respondents said the increased volume of transactions they can review using data analytics is very beneficial to their anti-fraud programs.



> While financial restrictions are a significant challenge for a large percentage of organizations when it comes to implementing new anti-fraud technology, 55% of the organizations in this study expect to increase their budgets for anti-fraud technology over the next two years—17% significantly and 38% slightly. Another 40% expect to have their budgets for such technology remain level. Only 6% of the organizations anticipate having their financial resources for anti-fraud technology reduced over the next two years, as demonstrated in the figure that follows:



Tips

Payroll fraud is classified as a form of asset misappropriation. In this scheme, an employee abuses his or her access to company payroll systems to issue unauthorized payments. According to the Association of Certified Fraud Examiners, payroll fraud is the number one source of accounting fraud and employee theft; a 2018 census showed that it occurs in 27% of all businesses.

Understanding how to prevent payroll fraud begins with understanding how it occurs. Some of the critical areas that should be validated, whereas their existence may indicate a weak internal control environment, are as follows:

> The absence of segregation of the duties of payroll set-up, approval, and processing functions.

> Terminated employees are not cleared-off / disabled from human resources and payroll registers.

> Poor controls over the process of creating and adding names to human resources and payroll registers.

> Limited oversight and control over the alteration of pay rates, and over the recognition of overtime hours and bonuses.

> Control weaknesses in capturing employee attendance data before payroll processing.

> The lack of a complete and comprehensive reconciliation exercise of the total monthly payroll payments, along with comparisons amongst successive periods.

> The absence of a formal documented policy and procedures manual for payroll matters, leading to the application of inconsistent practices by pertinent employees.

> The absence of linkage and interface between the grades for each position or job title as defined in the human resources management system with the system/ tool used by the Payroll Section, which allows that these grades be altered upon generating the monthly payroll register.

> No requirements for employees to take mandatory vacation time.

> Poor management of advances granted to employees.