ACCOUNTANCY EUROPE.

FIGHTING FINANCIAL CRIME

Auditor's role in the fight against fraud, corruption and money laundering

Information paper

FACTS.

AUDIT & ASSURANCE

DECEMBER 2017

HIGHLIGHTS

This information paper aims to clarify the auditor's role in fighting financial crime as to:

- deterrence
- detection
- communication and reporting

In an audit of financial statements (Audit), the auditor has clear and defined responsibilities in fighting financial crime. These responsibilities derive from International Auditing Standards (ISAs) and other specific laws and regulations aiming to combat financial crime. They also draw on fundamental principles of ethics and professional scepticism.

Audit may help deter potential wrongdoers and uncover financial crime. Nevertheless, tackling financial crime must be a joint effort of all relevant parties, including business leaders, the accountancy profession, regulators, standard setters and the financial sector.

TABLE OF CONTENTS

INTRODUCTION

Financial crime is harmful and has far reaching negative consequences. Victims range from individuals whose savings are depleted, to pension funds whose investments loose value. It also affects society as a whole when governments are defrauded, e.g. by corruption or tax evasion.

Perpetrators' modus operandi evolves rapidly, with advancements in technology opening up new avenues such as cybercrime. As a result, potential victims, including businesses, face emerging risks and need to adapt their behaviour and risk management accordingly.

When financial crime is reported in the press, the auditor's role may be called into question. With this paper, Accountancy Europe aims to clarify the auditor's role in fighting financial crime by taking a factual look at the role of the statutory auditor as one of the many parties cooperating in tackling financial crime.

This information paper is divided into seven parts. In the following background section, we define financial crime and look at its consequences through numbers. Afterwards, we provide an insight into how the ISAs deal with financial crime and explain what it means for the auditor's work. Then, in three core parts, we describe the statutory auditor's role in (i) deterring, (ii) detecting and (iii) communicating and reporting financial crime. In the conclusion, we sum up how the auditor contributes to combating financial crime.

BACKGROUND

WHAT IS FINANCIAL CRIME?

Financial crime covers fraud, corruption, bribery, money-laundering, insider trading, etc. There is no single internationally accepted definition of financial crime. Organisations like the International Monetary Fund (IMF) or the Organisation for Economic Co-operation and Development (OECD) interpret financial crime broadly, being an umbrella term for all non-violent crimes which result in a financial loss.[1]

In this publication, financial crime is considered in a wide sense that includes fraud, corruption and money laundering.

DEFINING FRAUD

Fraud is defined by the World Bank as "[…] any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation."[2]

The International Auditing and Assurance Standards Board (IAASB) describes fraud as "an intentional act by one or more individuals among management, those charged with governance (TCWG), employees, or third parties, involving the use of deception to obtain an unjust or illegal advantage."[3] Although fraud is a broad legal concept, the IAASB's ISAs[4] only deal with fraud which is a result of fraudulent financial reporting or misappropriation of assets.

DEFINING CORRUPTION

According to the World Bank, "A corrupt practice is the offering, giving, receiving or soliciting, directly or indirectly, anything of value to influence improperly the actions of another party."[5] This includes both active corruption, e.g. offering or giving a bribe, and passive corruption, e.g. receiving or soliciting a bribe.

---

[1] For further discussion on what financial crime is, refer, for example, to the IMF's publication *Financial System Abuse, Financial Crime and Money Laundering – Background Paper,* (2001)http://www.imf.org/external/np/ml/2001/eng/021201.pdf
[2] http://www.worldbank.org/en/about/unit/integrity-vice-presidency/what-is-fraud-and-corruption
[3] *2016–2017 Handbook of International Quality Control, Auditing, Review, Other Assurance, and Related Services Pronouncements* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[4] *ISA 240* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[5] http://www.worldbank.org/en/about/unit/integrity-vice-presidency/what-is-fraud-and-corruption

DEFINING MONEY LAUNDERING

Money laundering is the processing of criminal gains to disguise their illegal origin, including the complicity in the crime.[6]

Fraud and corruption are both predicate offences to money laundering. It means that these actions provide resources to be laundered. For instance, money received as a bribe can be transferred through the financial network in a way to appear to have originated from legal activities so that banks and other institutions deal with it without any suspicion. Due to this, the fight against fraud and corruption is intertwined with that against money laundering.

QUANTIFYING HARM

Crime affecting the European Union's (EU) financial interests has far reaching consequences and must be given great attention.

It is estimated that corruption costs the EU economy 120 billion EUR annually, which is just a little less than the entire EU budget.[7] Moreover, corruption distorts the business environment.[8] One of the findings of the Eurobarometer survey on corruption shows that at European level, more than four out of ten companies consider corruption to be a problem for doing business. According to the OECD, corruption can increase the cost of doing business by 10%.[9]

The Association of Certified Fraud Examiners' (AFCE) *Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study* (Global Fraud Study)[10] estimates that the financial losses caused by financial crime can be as high as 5% of revenues of an organisation each year. It also reveals that smaller organisations are more vulnerable to financial crime than large ones. Indeed, if they incur losses of the same amount it will likely make them feel much more the impact. Additionally, small organisations typically have fewer resources to combat this threat.

Financial crime also causes reputational damage to organisations involved, which may adversely affect their market value. These organisations also risk fines or other penalties from appropriate authorities.

INTERNATIONAL STANDARDS ON AUDITING AND FINANCIAL CRIME

OBJECTIVE OF AN AUDIT OF FINANCIAL STATEMENTS

According to the ISAs[11], the purpose of Audit is to enhance the degree of confidence of intended users in the financial statements. In conducting an Audit, the objective of the auditor is to obtain reasonable assurance about whether the financial statements, as a whole, are free from material misstatement due to fraud or error. This enables the auditor to express an opinion on whether the financial statements give a true and fair view in line with the financial reporting framework adopted by the audited entity.

---

[6] For a more detailed definition refer to the *Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES

[7] *EU Anti-Corruption Report,* (2014) https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/corruption/docs/acr_2014_en.pdf

[8] *Putting an end to corruption,* OECD, (2016) https://www.oecd.org/corruption/putting-an-end-to-corruption.pdf

[9] https://www.oecd.org/cleangovbiz/49693613.pdf

[10] https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

[11] *ISA 200* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

MATERIALITY

The concept of materiality relates to the significance of transactions, balances and errors in the financial statements. It is expressed as a monetary threshold. Based on the ISAs[12], misstatements, including omissions, are material if they could be expected to influence the economic decisions of users based on the financial statements.

HISTORICAL REASONS BEHIND THE CURRENT AUDIT APPROACH

As a result of an increase in volume and complexity of financial transactions, Audit is based on a reasonable assurance model. In order to apply it, a 'risk-based approach' to Audit has been introduced through the use of the ISAs. Fraud is always considered to be a significant risk demanding special audit consideration.[13]

In the planning of Audit, the auditor performs risk assessment procedures. This provides the auditor with a basis for the identification and assessment of the risks of material misstatement. Misstatements, including omissions, are material if they, individually or in the aggregate, could reasonably be expected to influence the economic decisions of financial statements' users.

Based on the risk assessment findings, the ISAs[14] require the auditor to perform audit procedures to address the risks in the individual engagement circumstances. With this approach, the auditor directs the work towards those risks and areas where it is more likely that fraud and errors in account balances or transactions would result in a material misstatement of the financial statements.

RECENT CHANGES IN INTERNATIONAL STANDARDS

In Audit, the auditor has clear and defined responsibilities relating to fraud. The terms 'corruption', 'financial crime' and 'money laundering' have been specifically introduced in the revision of ISA 250 to align it with the project of the International Ethics Standards Board for Accountants (IESBA) related to non-compliance with laws and regulations (NOCLAR).[15]

NOCLAR sets out requirements and provides guidance to auditors and other professional accountants on how to act in the public interest when they become aware of a suspected illegal act committed by a client or employer. NOCLAR provisions cannot override specific national legislation governing the auditor's role. This initiative intends to raise the ethical bar for the auditor and enhance the auditor's role in the fight against financial crime. However, notwithstanding the auditor's objective to obtain reasonable assurance about whether the financial statements are free from material misstatement due to fraud or error, detection of financial crime per se is not the primary focus of Audit.

INHERENT LIMITATIONS OF AUDIT

Due to the inherent limitations of Audit, the auditor is not expected to and cannot obtain absolute assurance that the financial statements are free from material misstatement, whether due to fraud or error. The combination of the inherent limitations of Audit and the application of the principle of materiality reduces the auditor's ability to detect fraud, especially where the impact is immaterial to the financial statements.

---

[12] *ISA 320*, https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[13] For risks that require special audit consideration refer to *ISA 315 (Revised)* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[14] *ISA 330* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[15] More information on the IESBA's NOCLAR project is available at https://www.ethicsboard.org/responding-non-compliance-laws-and-regulations

According to the ISAs[16], the inherent limitations of Audit are linked to:

- **The nature of financial reporting**

It includes, for example, the use of judgement in determining accounting estimates which creates space for possible inaccuracies. It is important to note that estimation uncertainties cannot be eliminated by applying additional audit procedures.

- **The nature of audit procedures**

The auditor does not test all transactions, but uses sampling methods to select transactions and balances for audit testing. There is therefore an inherent risk that the audit procedures, although carried out appropriately using representative samples, may fail to detect a material misstatement in the financial statements.

A limitation on the auditor's ability to obtain audit evidence may stem, for example, from the possibility that management or others do not provide complete information relevant for the preparation of the financial statements or as requested by the auditor. As a result, the auditor cannot correctly assess the completeness of the information.

Audit procedures used to gather audit evidence may be ineffective for detecting an intentional misstatement due to sophisticated arrangements designed to conceal fraud, e.g. falsified documentation given to the auditor.

- **The need for Audit to be conducted within a reasonable period of time and at a reasonable cost**

This sets the limit for the auditor in terms of audit procedures carried out. The auditor has to prioritise tasks essential for the effective performance of Audit.

The ISAs recognise that there are other matters that affect the inherent limitations on the auditor's ability to detect material misstatements. These matters include:

- the nature of fraud, particularly when senior management is involved
- the existence and completeness of related party relationships and transactions
- the occurrence of non-compliance with laws and regulations
- future events or conditions that may cause an entity to cease to continue as a going concern

To assist in mitigating the effect of these inherent limitations, specific audit procedures are identified in relevant ISAs[17].

PROFESSIONAL SCEPTICISM

Maintaining professional scepticism throughout Audit is very important in the context of the auditor's role in detecting fraud. The auditor shall keep in mind that the risk of not detecting a material misstatement resulting from fraud is higher than the risk of not detecting one due to error.[18]

Fraud is usually devised in a sophisticated way and often involves collusion. Perpetrators will generally go to great lengths to conceal it from the auditor. ISA 240 makes the auditor aware that the risk of not detecting a material misstatement resulting from management fraud is greater than one from an employee fraud. This is due to management being in a position to manipulate accounting records, present fraudulent financial information or override controls.

[16] *ISA 200* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[17] *ISA 240, ISA 550, ISA 250 (Revised)* and *ISA 570 (Revised*)
[18] *ISA 240* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

ETHICAL REQUIREMENTS

Besides applying the ISAs, the auditor has to comply with relevant ethical requirements, including those relating to independence. These ethical requirements are included in national legislation or professional standards that are ordinarily based on the IESBA Code[19]. Application of the fundamental principles of ethics[20] is a prerequisite in the audit process to be able to critically assess audit evidence, including suspected financial crime by a client.

QUALITY CONTROL FOR AUDITS

Audit firms have to comply with ISQC 1[21] quality control requirements for Audits. Audit firms are required to have an internal system of quality control policies and procedures that is subject to public oversight when applicable. It ensures that all Audits are conducted in accordance with the ISAs and other applicable requirements. This safeguards consistency and quality in Audit.

DETERRING FINANCIAL CRIME

The management, together with the oversight of TCWG, are responsible for the integrity of the organisation and for preventing incidents of financial crime involving their organisation.

Audit helps deter financial crime when performing the following procedures:

- accepting an audit client
- obtaining an understanding of the entity and its environment

ACCEPTING AN AUDIT CLIENT

Auditors are required to follow specific rules and procedures when accepting a new client or reassessing a relationship with an existing client.

INTERNATIONAL STANDARDS ON AUDITING

The ISAs[22] require the auditor to accept a new client or to continue a relationship with an existing client based on conclusions of appropriate procedures. Within this process, the auditor shall consider the integrity of the client. This includes any indications that the client might be involved in money laundering or other criminal activities.[23]

Information sources on the integrity of the client may include communications with existing or previous providers of accountancy services to the client, inquiries of employees and discussions with other third parties.

The auditor should also consider significant matters that have arisen during the current and previous audit engagements and their implications for starting or continuing the relationship.

Unless prohibited by law or regulation, the proposed successor auditor may request that the predecessor auditor provides information relating to identified or suspected non-compliance with laws and regulations.[24]

---

[19] We refer to Parts A and B of *the IESBA Code* https://www.ethicsboard.org/iesba-code
[20] Integrity, objectivity, professional competence and due care, confidentiality and professional behaviour as per *the IESBA Code* https://www.ethicsboard.org/iesba-code
[21] https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[22] *ISA 220* and *ISQC 1* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
Note: In line with the new requirements in *the Code of Ethics for Professional Accountants* (the IESBA Code) addressing non-compliance with laws and regulations, the IAASB has made amendments to *ISA 250* and to other applicable International Standards. *ISA 250 (Revised)* and the conforming amendments to other standards become effective for Audits of periods beginning on or after 15 December 2017. In this publication, we refer to *ISA 250 (Revised)* and consider the conforming amendments https://www.ifac.org/system/files/publications/files/IAASB-NOCLAR-ISA-250-Revised-and-Related-Conforming-Amendments-Oct-2016.pdf
[23] *ISQC 1* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[24] *IESBA Code* https://www.ethicsboard.org/iesba-code

THE EU ANTI-MONEY LAUNDERING DIRECTIVE[25]

Money laundering and terrorist financing, and assisting in such activities, are criminal offences in all EU Member States.

The auditor has to meet specific obligations which derive from the criminalisation of these activities as set out in the EU Anti-Money Laundering Directive (the AML Directive). The AML Directive aims to strengthen the EU's defences against money laundering and terrorist financing.

The auditor has to carry out Customer Due Diligence (CDD) when:

- accepting a new client or reassessing a relationship with an existing one
- suspecting money laundering or terrorist financing by a client
- having doubts about the veracity of previously obtained client identification data

CDD comprises:

- identifying and verifying the client's identity, its beneficial owner, and each person acting on behalf of the client
- assessing the purpose and nature of the business relationship
- ongoing monitoring

Audit firms cannot establish a business relationship and have to terminate an existing business relationship with a client if they cannot comply with the CDD requirements. For example, audit firms cannot accept a client when they cannot verify the beneficial owner of that client. However, there are a few exceptions to this rule.

The auditor needs to carry out enhanced due diligence measures in cases of high risk. For example, senior management approval is required for accepting a client that is a Politically Exposed Person.

The identification of the beneficial owner is likely to become easier than before. Member States are now required to ensure that beneficial owner information is held in a central register. Audit firms will have access to these registers within the framework of CDD. However, audit firms cannot rely exclusively on the register to fulfil their CDD obligations.

The AML Directive is currently being revised as part of the EU's response to the Panama Papers' scandal and the terrorist attacks across Europe in 2015 and 2016.

UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT, INCLUDING INTERNAL CONTROLS

The auditor cannot directly prevent financial crime from happening, but the auditor can tailor the audit work to increase the chance of detecting it.

By obtaining an understanding of the entity and its environment, including its internal controls, the auditor may identify areas susceptible to fraud. Based on this understanding, the auditor can then design further appropriate audit procedures. However, it is up to management to duly address a potential issue.

INTERNATIONAL STANDARDS ON AUDITING: UNDERSTANDING THE ENTITY AND ITS ENVIRONMENT

Based on the ISAs[26], the auditor is required to identify and assess the risks of material misstatement due to fraud or error. This assessment is done through obtaining an understanding of the audited entity and its environment, including the entity's internal controls.

---

[25] *Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AML Directive)* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:JOL_2015_141_R_0003&from=ES

[26] https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

The auditor shall obtain[27], for example:

- an understanding of the entity's industry and business model
- its long-term objectives
- the applicable regulatory and corporate reporting framework
- the ownership and governance structures
- the measurement and review of the entity's financial performance

Examples of audit procedures for obtaining an understanding of the entity's internal control relating to laws and regulations on corruption

The auditor obtains an understanding of the audited entity's anti-corruption compliance programme, including the presence of a code of conduct, how it is implemented, how its efficiency is monitored.

Based on this understanding, for example, the auditor may need to assess specific internal procedures for screening of intermediaries, for dealing with business gifts or for authorising invoices of intermediaries and agents.

INTERNAL CONTROLS

(I) INTERNATIONAL STANDARDS ON AUDITING

According to the ISAs[28], the auditor shall obtain an understanding of the entity's internal controls relevant to Audit.[29] These mainly relate to the segregation of duties, authorisation, information processing, performance reviews and physical controls. The auditor shall then evaluate the design of these controls and, by performing appropriate audit procedures, determine whether the controls operate effectively and so can be relied upon.[30]

If the auditor has determined in the risk assessment that a significant risk exists, the auditor has to obtain an understanding of the entity's controls relevant to that risk.[31] In case an entity has a risk assessment procedure in place, the auditor evaluates the entity's management of risks, which could include fraud, and the measures taken to mitigate these risks.[32]

The auditor shall obtain an understanding of the information system (IT), including the related business processes, relevant to financial reporting.[33] Additionally, the auditor shall obtain an understanding of how the entity has responded to risks arising from IT and take it into account when assessing the risk of material misstatement in the financial statements.

Cybercrime is a major risk to be considered as organisations and businesses are increasingly susceptible to this type of attack. It is a criminal activity which involves computers, networks, programmes and data. A breach in cybersecurity is often targeted towards identity or data theft, transaction fraud, system outage, etc. and causes financial and reputational harm, diminished investor confidence and regulatory fines. A pervasive approach helps develop protective mechanisms. Entities should be aware of cybercrime methods to adapt their control environments. The auditor is required to obtain an understanding of the entity's internal control

---

[27] In June 2017, the European Commission for the first time released its *Supranational Risk Assessment Report* which assesses the vulnerability of financial products and services to risks of money laundering and terrorist financing. The analysis can serve as an important source of information also for auditors. Identification of potentially risky sectors, operations and territories could prove useful in the auditor's understanding of the audited entity. The report is available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=81272

[28] *ISA 315 (Revised)* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

[29] Note: Please refer to *ISA 315 (Revised)* for a description of 'controls relevant to Audit'.

[30] For details related to the testing of controls please refer to *ISA 330* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

[31] *ISA 315 (Revised)* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

[32] Please refer to *ISA 330* for details https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

[33] *ISA 315 (Revised)* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf

environment and risk assessment processes, and is in a position to alert the entity, should there be deficiencies in this area.

Example of data breach and the implications for the auditor

An audited entity has been hacked and the data in the accounting system could have been changed. There is no back-up of the data.

The auditor will need to consider what impact this incident has on the financial statements' integrity and whether any action needs to be taken.

(II) LINK WITH EMPIRICAL EVIDENCE

The findings of the ACFE's Global Fraud Study[34] demonstrate a positive impact of certain internal controls on combating financial crime. The presence of anti-fraud and anti-corruption internal controls is correlated with lower losses for an organisation and quicker detection of incidents of financial crime. Based on the study, the following controls have proven to be the most effective:

Ten most effective controls in terms of reducing losses from fraud or corruption	Ten most effective controls in terms of reducing the duration of fraud or corruption
Proactive data monitoring/analysis	Surprise audits
Management review	Proactive data monitoring/analysis
Hotline	Dedicated fraud department/function/team
Management certification of financial statements	Hotline
Surprise audits	Formal fraud risk assessments
Dedicated fraud department/function/team	Management review
Job rotation/mandatory vacation	Independent audit committee
External audit of internal controls over financial reporting	Internal audit department
Fraud training for managers/executives	External audit of internal controls over financial reporting
Fraud training for employees	Management certification of financial statements

These findings could be taken into consideration by the auditor, especially in the planning phase of Audit when the risk assessment is carried out. If the audited entity has well-functioning controls to prevent and detect fraud, the risk of fraud can be effectively lowered.

DETECTING FINANCIAL CRIME

Detecting fraud is the responsibility of the management of the entity, together with the oversight of TCWG. It is also their responsibility to make sure that the entity complies with applicable laws and regulations.

The auditor's work in this context is very challenging and requires professional scepticism to be duly exercised. Ultimately, it is up to a court to determine whether a criminal act has been committed.

[34] https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

INTERNATIONAL STANDARDS ON AUDITING

THE AUDITOR'S RESPONSIBILITIES RELATING TO FRAUD

In Audit, based on the ISAs[35], the auditor is concerned with fraud that causes the financial statements to be materially misstated. The auditor is responsible for obtaining reasonable assurance that the financial statements as a whole are free from material misstatement, whether due to fraud or error. As already noted, the term 'fraud' and the associated auditor's responsibilities in the ISAs only refer to fraud as a result of fraudulent financial reporting or misappropriation of assets.[36]

CONSIDERATION OF LAWS AND REGULATIONS IN AUDIT

The requirements in the ISAs[37] are designed to assist the auditor in identifying material misstatements in the financial statements due to fraud and error, including non-compliance with laws and regulations that the audited entity is subject to. National legislation on corruption and money laundering is part of the laws and regulations to be considered by the auditor in this context.

The ISAs[38] distinguish between two types of laws and regulations:

1. With a direct effect on the determination of the material amounts and disclosures in the financial statements, such as tax and pension legislation. For this category, the auditor is required to obtain sufficient appropriate audit evidence regarding compliance.
2. Without a direct effect: in this case, compliance may be fundamental to the operating aspects of the business, to an entity's ability to continue its business, or to avoid material penalties. The auditor's responsibility in this category of laws and regulations is limited to specified audit procedures to help identify non-compliance that may have material effect on the financial statements.

Corruption and money laundering are illegal acts as defined in national laws of EU Member States. Therefore, audited entities may face material penalties in case of non-compliance with these laws and regulations. Specified audit procedures shall address the identification of such non-compliance.[39]

Based on the ISAs[40], if the auditor becomes aware of information on non-compliance with laws and regulations, the auditor shall obtain an understanding of the nature of the act and the circumstances in which it has occurred. The auditor shall also obtain further information to evaluate the possible effect on the financial statements.

The ISAs[41] have now listed anti-corruption and anti-money laundering legislation as one of the categories of laws to be considered by the auditor when assessing compliance. In addition to this, a newly included definition of non-compliance gives bribes' acceptance as an example of non-compliance. When the auditor detects non-compliance with anti-corruption laws, regardless of materiality, the auditor shall consider what impact this has on other aspects of Audit, especially when the integrity of management is in question.

---

[35] *ISA 240* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[36] *ISA 240* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[37] *ISA 250 (Revised) and related Conforming Amendments* http://www.ifac.org/system/files/publications/files/IAASB-NOCLAR-ISA-250-Revised-and-Related-Conforming-Amendments-Oct-2016.pdf
[38] *ISA 250 (Revised)* http://www.ifac.org/publications-resources/isa-250-revised-consideration-laws-and-regulations-audit-financial-statements
[39] *Ibidem*
[40] *Ibidem*
[41] *Ibidem*

Example of further investigation in the course of Audit

During an interview with the auditor, an employee blows a whistle on how a specific contract with a public-sector organisation has been secured advantageously for the audited entity. This is indicative of fraud and corruption.

The auditor needs to follow up on such indications. Where accusations are substantiated, the auditor can further examine the contract and the related project accounting records or specific expense accounts, as well as conduct further interviews or analytical procedures.

The auditor would seek to understand whether any non-compliance with laws and regulations has occurred and to what extent. The auditor shall communicate any conclusion to the right level of the organisation, either to management or TCWG, depending on the particular engagement circumstances.

DETECTING FINANCIAL CRIME – LINK WITH RECENT DEVELOPMENTS

NON-FINANCIAL INFORMATION REPORTING

A new requirement for large PIEs[42] to disclose non-financial information (NFI)[43] includes reporting on anti-corruption and bribery issues. The auditor is required to check that this information is reported by the audited entity, i.e. an existence check.

NFI is deemed more and more important by various stakeholders, including investors. To be perceived as reliable information and to respond to the market demand, we can expect that NFI reporting will undergo a transformation in the coming years. In this process, we can expect organisations to develop criteria for performance evaluation and internal controls relating to corruption and bribery. The final step could be the verification of the reported information and the control systems in place by an assurance practitioner, offering new means to tackle corruption and bribery.

WHISTLEBLOWING

According to the ACFE's Global Fraud Study[44], whistleblowing[45] is the most common detection method of financial crime. Over 39% of financial crime cases examined in the study were initially detected thanks to a tip from a whistleblower.[46] Furthermore, the findings show that organisations that have reporting hotlines are much more likely to detect financial crime through tips than organisations without them.

In comparison, less than 4% of examined cases have been uncovered through audit procedures. This is in line with the fact that Audit is not designed specifically to detect financial crime. Whistleblowers can tip off low value financial crime that would not be on the auditor's radar due to materiality, inherent limitations or lack of relationship to the financial statements.

This emphasises the importance of having well-functioning whistleblowing mechanisms and supporting legislation in place.

---

[42] Applies to large PIEs with more than 500 employees. The scope includes approximately 6 000 companies across the EU. More information available at https://www.accountancyeurope.eu/wp-content/uploads/1512_EU_Directive_on_NFI.pdf

[43] *The EU Directive on disclosure of non-financial information and diversity information (2014/95/EU)*http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014L0095&from=EN

[44] *Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study*; https://www.acfe.com/rttn2016/docs/2016-report-to-the-nations.pdf

[45] Understand as tips received from employees as well as customers, suppliers and other parties.

[46] Over half of these tips were received from employees, which is generally the focus of reporting mechanisms at most organisations. However, organisations as well as the auditor need to take into account that 40% of all tips came from non-employees, which demonstrates the need for a reporting mechanism for both internal and external sources of tips. The study suggests that promoting reporting mechanisms to multiple audiences might result in receiving more tips and therefore decreasing the risk of undetected financial crime.

The European Commission is currently assessing the scope for horizontal or further sectoral action at EU level to strengthen the whistleblower protection. This should help protect the European economy against organised crime, fraud, corruption and money laundering.[47]

IMPACT OF NEW TECHNOLOGIES

With all the possibilities that new technologies offer nowadays, auditors may determine that it is appropriate to use them also in respect of detecting fraud during Audit.[48]

COMMUNICATING AND REPORTING FINANCIAL CRIME

Auditors play a role in communicating and reporting financial crime.

COMMUNICATING

INTERNATIONAL STANDARDS ON AUDITING[49]

The auditor is required to discuss identified or suspected fraud or non-compliance with legislation with management and if appropriate, with TCWG. However, the ISAs[50] emphasise that communication with management or TCWG might be restricted or prohibited by law in certain cases. The reason is that it could serve as a warning for the audited entity and, therefore, prejudice the investigation by an authority, i.e. legislation may preclude tipping-off in some jurisdictions.

The auditor has to evaluate the effect of suspected or identified fraud or non-compliance on the audit opinion in line with the ISAs. In certain cases, the auditor may determine that the identified or suspected non-compliance is a Key Audit Matter (KAM) that needs to be included in the audit report in accordance with the ISAs[51].

Communicating KAMs[52] enhances the informative value of the audit report. It improves transparency and enhances understandability of both the audit report and the matters surrounding the audited entity. The auditor may communicate financial crime as a KAM in the audit report if it is perceived as a key risk by the auditor.[53]

REPORTING

If the auditor identifies or suspects non-compliance by a client, the auditor has to determine whether[54]:

- law, regulation or relevant ethical requirements require reporting to an appropriate authority outside the entity
- national legislation prohibits reporting to an authority as a breach of client confidentiality

Whether an act constitutes non-compliance cannot be determined by the auditor. This is ultimately decided by a court or other relevant authority.

The EU audit and AML legislation requires the auditor to report financial crime in certain situations.

---

[47] *Horizontal or further sectorial EU action on whistle-blower protection* http://ec.europa.eu/smart-regulation/roadmaps/docs/plan_2016_241_whistleblower_protection_en.pdf
[48] *ISA 330* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[49] Based on *ISA 240* and *ISA 250 (Revised)* http://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[50] *ISA 250 (Revised)* and *ISA 240*
[51] *ISA 701* https://www.ifac.org/system/files/publications/files/2016-2017-IAASB-Handbook-Volume-1.pdf
[52] Applicable to PIEs according to the 2014 Audit Regulation available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0537&from=EN and applicable to listed entities based on ISA 701https://www.iaasb.org/system/files/publications/files/ISA-701_2.pdf
[53] Rolls-Royce's 2015 and 2016 audit reports include examples of the auditor's response to the investigation relating to an incident of corruption involving the entity. The full 2016 report is available here https://www.rolls-royce.com/~/media/Files/R/Rolls-Royce/documents/investors/annual-reports/2016-annual-report.pdf
[54] *ISA 250 (Revised)* http://www.ifac.org/publications-resources/isa-250-revised-consideration-laws-and-regulations-audit-financial-statements

EU AUDIT LEGISLATION[55]

The statutory auditor of a PIE is required to promptly report to the competent authorities any information concerning a client which may bring about any of the following:

- a material breach of laws, regulations or administrative provisions
- a material threat or doubt concerning the continuous functioning of the entity
- a refusal to issue an audit opinion or the issuing of an adverse or qualified opinion on the financial statements
- any additional information that is deemed necessary for effective financial market supervision, as provided for in applicable national law

This type of disclosure to the competent authorities by the statutory auditor does not constitute a breach of any contractual or legal restriction on disclosure of information.

THE EU ANTI-MONEY LAUNDERING DIRECTIVE

Based on the EU's AML Directive, the auditor has an obligation to report suspicious activities by a client to a national Financial Intelligence Unit or to a designated self-regulatory body. Suspicious activities include both transactions, attempted transactions and patterns of transactions or behaviour.

In Audit, the auditor is not specifically required to look for money laundering and terrorist financing, but to report suspicion of such activities. The suspicion threshold is relatively low; auditors are already required to report when they have reasonable grounds to suspect money laundering or terrorist financing.

The materiality concept used in Audit is not applicable in the context of money laundering. Therefore, the auditor has to take into account that a transaction of any size can be the subject of money laundering and terrorist financing. Money can be laundered using numerous low value transactions. For this reason, the auditor cannot assume that a report is not required because the individual value of a transaction is low.

CONCLUSION

The role of the statutory auditor in fighting financial crime, including fraud, through Audit is defined by auditing standards and applicable legislation. Audit may help deter potential wrongdoers and uncover financial crime even though this is not its primary focus.

Audit contributes to combating financial crime as follows:

- the auditor is required to alert TCWG of the audited entity, and may also decide to communicate incidents of fraud or non-compliance in the audit report
- if not prohibited by law, the auditor may deem it appropriate to report incidents of financial crime to an appropriate external authority
- the auditor is required to report suspicions of money laundering and terrorist financing by a client

Successfully tackling financial crime depends upon a joint effort by all relevant parties, including business leaders, the accountancy profession, regulators, standard setters and the financial sector. We call for a coordinated approach and commitment of all the key players to achieve tangible results.

Technology offers new opportunities for combating financial crime. Accordingly, the accountancy profession is committed to developing data analytics tools and new skillsets needed for this area.

[55] *Regulation (EU) No 537/2014* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32014R0537

Avenue d'Auderghem 22-28, 1040 Brussels

+32(0)2 893 33 60

www.accountancyeurope.eu

@AccountancyEU

Accountancy Europe

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 50 professional organisations from 37 countries that represent **1 million** professional accountants, auditors and advisors. They make numbers work for people. Accountancy Europe translates their daily experience to inform the public policy debate in Europe and beyond.

Accountancy Europe is in the EU Transparency Register (No 4713568401-18).