DISCUSSION PAPER

10 HOT TOPICS FOR THE 2017 INTERNAL AUDIT PLAN

The Institute of Internal Auditors
France
Italy
Spain

HOT TOPICS INDEX

Acknowledgments

Many people have helped with the preparation of this document. In particular we would like to thank chief internal audit executives from different industries (banking, insurance, chemical, energy, public sector, distribution and construction) who have shared with us their vision and challenges as internal audit leaders for the future of our profession.

PROLOGUE

OPPORTUNITIES AND RISKS EVOLVE CONTINUOUSLY as organisations and their environments change. Inherently, anticipating the consequences of these emerging risks and opportunities, and their ramifications, can be challenging.

With this new report, our objective is to help rationalise and categorise these risks and opportunities, and in turn provide actions for **Heads of Internal Audit.** It is not intended to be a reference but rather a basis for a discussion that we want to open with our members, a tool at your disposal to help understand the next challenges for our profession.

To ensure its pertinence, we used diverse sources of information including reports from international institutions and advisory firms and interviews with **Heads of Internal Audit** across Europe.

With your help, through our discussions and in response to the evolving business environment, we will periodically release updated versions of this list of hot topics.

This paper has been produced by IFACI, IIA Italy, IIA Spain and with the support of the Chartered Institute of Internal Auditors (UK and Ireland).

We will come back to you shortly to start this conversation and we would welcome your comments and reactions.

TOPIC 01

GEOPOLITICS

Some of the most worrying risks for any national or international organisation are of a geopolitical nature.
Some organisations may see geopolitical risks as too complex to deal with internally. Any business that operates outside its home needs a strong understanding of geopolitics.
We live in a VUCA world (volatile, uncertain, complex and ambiguous) according to the acronym coined at the US Military War College in the early 1990s, and this remains valid today.

In June 2016, the World Bank Group published its most recent **Global Economic Prospect,** detailing its assessment of current risks and divergences. The risks defined in this document coincide with those that had been identified in the publication 25 years ago:

"Today, rising uncertainties from different, yet related, directions portend difficulties to come... Individually, none of these dark economic clouds would be sufficient to dampen the short-term prospects for the world economy. But together they present compelling evidence that the world economy is in for a turbulent period in the short term. [1]

"... The impact of external circumstances on developing countries will depend crucially on how individual countries manage these contingencies. Policies in industrial countries will need to be sensitive to the concerns of "emerging and

developing countries and make it easier for them to restore momentum to the growth process. This would be especially important for low-income countries that have relatively few strategic options open to them for sustained development".[1]

Asia and the increase in competitiveness

Globalisation means that the world's economies cooperate and trade goods like never before. This has brought some major benefits but has also led to several drawbacks that are tough to manage.

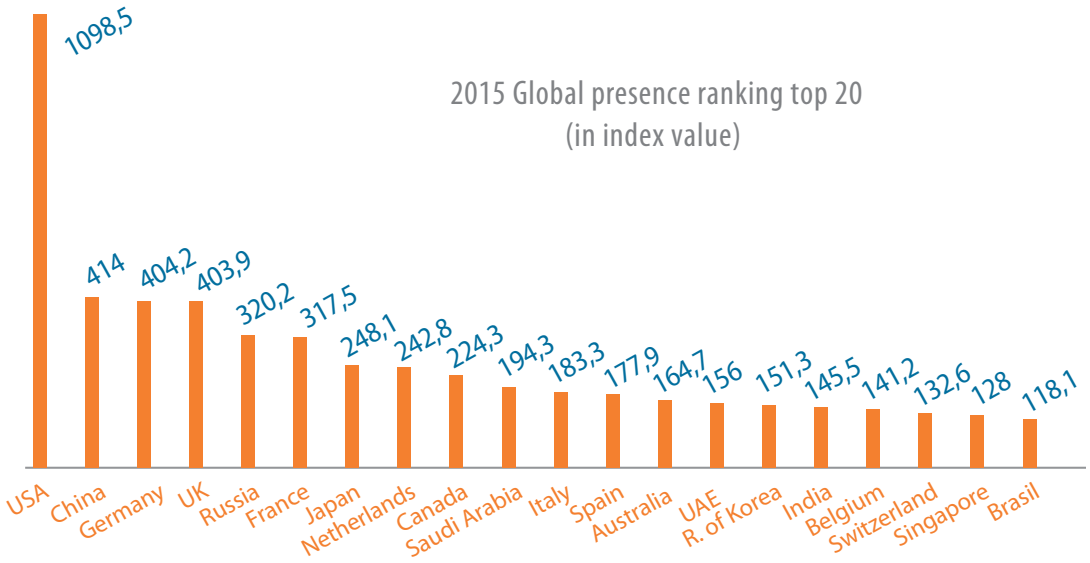
For example, the incorporation of four billion Asian people into the labour market had consequences four every country around the world, with significant movements in terms of production centres and an unprecedented increase in competitiveness. This was a decisive factor for many organisations as they were left high and dry after failing to go international.

The 2016 edition of the **Elcano Global Presence Index** (drawn up from the results of a survey conducted in 2015 on international experts) lists 90 countries according to the degree to which they are involved in the globalisation process. [2]

This year's edition highlights China's position in second place on the global presence index, the stagnation of the globalisation process and how the collapse of raw material prices is affecting the economies of emerging nations.

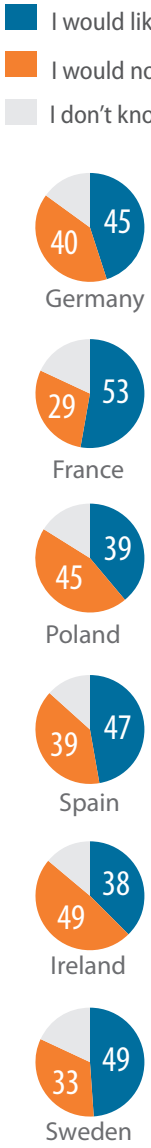
These factors and many others are leading to an increase in risks and a greater risk likelihood in geographic areas that we did not anticipate, making it difficult to quantify the economic impact for the organisation.

These factors and many others are leading to an increase in risks and a greater risk likelihood in geographic areas that we did not anticipate, making it difficult to quantify the economic impact for the organisation.



Source:
Real Instituto Elcano

Wish for own country to hold similar referendum as Britain by country (%)



Source: University of Edinburgh

Europe: Fracture worsened by Brexit?

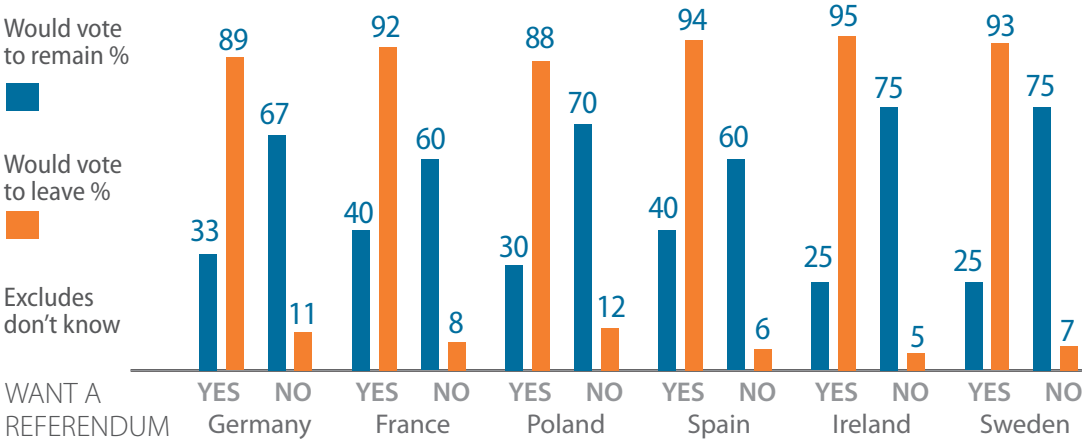
In the case of Europe, a relatively stable and secure region, the situation has changed in recent years.

The decision taken by the United Kingdom to leave the European Union (BREXIT) was a genuine surprise for many organisations. The European project is now in doubt due to the accumulation of various crises within the union that have not been resolved satisfactorily, and Brexit is casting doubt over the validity of the European model as a whole.

There are concerns over a contagion effect and such studies as The view from the continent: What people in other member states think about the UK's EU referendum, conducted in June 2016 by The University of Edinburgh [3], provides some worrying figures. Up to 53% of French would like a referendum today on whether their country should remain in the EU and Marine Le Pen has already promised this will happen if she is president in 2017. The French are closely followed in this sentiment by the Swedish (49%), the Spanish (47%) and the Germans (45%).

The Euro crisis led to opposing views between the north (creditor) and the south (debtor), and the refugee crisis has opened a divide between the east and the west of Europe. The failed coup d'état in Turkey and the Jihadi attacks in various European countries are affecting the stock markets and various sectors of the economy, with tourism being a clear example of the sectors most sensitive to these crises. According to the French Foreign Affairs Minister, it is estimated that Paris has lost one million tourists and a billion euros in the first six months of the year due to the recent attacks. [4]

Preferences if a referendum on own country's membership in the EU were to be held by wish for own country to hold a referendum by country (%)



This European weakness has led to the publication of A Global Strategy for the European Union's Foreign and Security Policy in June 2016, given that political instability leads to an outflow of capital and is not attractive for investment. [5]

Main risks to be included in the risk map

It is no surprise that geopolitical risks condition international expansion, continued operations in a country and reassessment of the risks that could suspend investment, and they should be properly identified and managed.

The following geopolitical risks can be found on any risk map:

Political risk. Changes in government, dictatorships, nationalisations, wars and trade sanctions are risks to be considered when an organisation establishes itself in a country.

Regulatory risk. Hot topic for this document. The enormous complexity of this risk, with specific sectorial, labour and constantly changing regulations has meant that organisations need to equip themselves with specialised resources.

Tax risk. The organisation not only has to meet its legally imposed tax obligations but must also consider its image in terms of fiscal optimization as this could have negative repercussions vis-a-vis the various stakeholders and could be penalised with a reduction in sales or even a loss of customers.

A recent example of this can be found in Apple and the European Commission's opinion that Apple benefited from illegal tax breaks in Ireland for years (2003 to 2014). Apple was forced to retroactively pay all the money it had avoided paying, plus the corresponding interest, estimated at over 13 billion euros. Ireland may appeal the sanction (which is the actual beneficiary of that money) and if that amount is collected, the tax rulings applied will recognise that they are illegal as well as those it has with other companies.

With Europe's backing on this issue, it is possible that countries might decide at an individual level to investigate whether this or other organisations also owe taxes. Portugal has already announced investigations and has opened the debate on whether Europe needs to revise its policies and limit the fiscal powers of Member States.

Exchange rate risk. The devaluation or appreciation of a currency has important repercussions on the income statement, especially in import/export operations. A currency devaluation also affects the margins and, depending on the subsidiary/parent company weighting, the consolidated income statement.

Liquidity risk. Any organisation or international investor might need to increase its liquidity at any given moment by liquidising its investments, and any restriction on this from the country could pose a serious risk.

Legal risks. The independence of the legal system is questionable in numerous countries, as is its efficiency. When entering into a

Brexit is casting doubt over the validity of the European model as a whole

Head of Internal Audit must consider their impact on the organisation by performing stress tests for the various scenarios and lending maximum support to senior management for business continuity and investment strategies

legal process in some countries, this can be slow and not always fair.

It is worth highlighting Spain and Italy, for example in this regard, where there is not only the possibility of an administrative penalty but there is also the chance of criminal liability for the organisation, which could lead to the closure of the company and legal action being brought against some of the executives in the most extreme cases.

Corruption risks. Although this risk is regulated in order to minimise it as far as possible, it is a reality in numerous countries due to political inefficiencies and a lack of ethical values among staff of the public administration services and members of the organisation.

Energy/raw material/supply risks. The energy dependency of a country or lack of raw materials is a highly important factor. Europe, as the main Russian gas customer, is an example of this. A third of European needs are covered by Russian gas. Half of these gas imports travel through Ukraine, which is in conflict with Russia due to the Russian annex-ation of the Crimean Peninsula. For some countries, such as Finland, the Baltic States and the Czech Republic, Russian gas imports account for a quarter of all the energy they consume.

The price is another decisive factor. The economic turmoil caused by the falling price of crude - for Venezuela, for example - is enormous because its economy depends on the revenue from this energy source. Russia is also experiencing difficulties; it drew up its budget for 2016 based on a price of 50 dollars per barrel.

The role of the Head of Internal Audit in terms of these risks

All these interconnected, complex and volatile variables mean that the **Head of Internal Audit** must consider their impact on the organisation by performing stress tests for the various scenarios and lending maximum support to senior management for business continuity and investment strategies.

The document published by the IIA Global in May 2015, **Grappling with Geopolitics,** assigns the role of assessing and advising on the capability of organisations to foresee geostrategic risks to Internal Audit.

We should examine how it may affect our capacity to achieve targets. For this reason, it is recommended that Internal Audit functions have a local presence in the areas they intend to examine in order to thus have sufficient knowledge and local experience.

As stated by **Ernesto Martinez, Chairman of IA Spain,** in the article entitled *"El imperativo de la Resiliencia",* companies must continue developing and researching in order to be resilient to change and contribute to their own stability.

The most relevant factor for determining the final impact on organisations will be the risk control and management system implemented by each company. Hence, the internal auditor must try to strengthen these two fundamental pillars.

TOPIC 02

GOVERNANCE

Events of recent years have clearly demonstrated the enormous importance of proper oversight of corporate governance at organisations.
Good corporate governance is directly related to the value attributed to an organisation by society and investors. The short-term benefits no longer hold such great importance and other aspects besides those associated with the income statement are now valued more highly.
We need to recognise that most problems at organisations have arisen due to weaknesses in their corporate governance and rarely has it been possible for the internal auditor to identify them.

THE VERY DEFINITION of internal auditing states that risk management, control and governance process effectiveness must be improved, but the internal auditor has never felt comfortable with this last process.

In its International Standards, the IIA Global defines corporate governance as follows:

"Governance is the combination of processes and structures implemented by the board in order to inform, direct, manage and monitor the activities of the organisation toward the achievement of its objectives."

There are many examples to be found of scandals involving corporate governance that affect all parts of the world and all kinds of organisations.

In 2012, **JP Morgan Chase** lacked Directors with sufficient expertise on its Risks Committee, a shortcoming that was only corrected after Bruno Iksil made a six billion-dollar loss in trading.

It is key to speak with other people in key governance positions within the organisation as this can clarify the knowledge held by the Head of Internal Audit

In Brazil, Petrobras was involved in a bribery and money laundering scandal after transferring hundreds of millions of dollars into the pockets of employees, contractors and politicians, among them Dilma Rousseff herself. It affected over 40 politicians who participated in an extensive bribery scheme.

One of the most well-known cases in Spain is that of the "Black Cards" at **Caja Madrid** (no longer in business), opaque cards that were handed out to 86 members of the board and executives at the bank who managed to skim up to 15 million euros as personal expenses.

The role of Internal Audit

It is generally thought that corporate governance only applies to listed companies, whereas it is precisely unlisted companies that most need good corporate governance.

When the **Head of Internal Audit** reviews this area, he is going to touch on highly sensitive issues (transparency, remunerations, etc.) and, more often than not, these issues are also kept confidential from other employees (such as the strategic plan).

The great responsibility of the Head of Internal Audit is to provide members of the board of directors with guarantees on **due diligence in their roles of overseeing the governance, risks and control system (GRC),** because they need to know that risks are being managed and controlled correctly and that the operational decisions reached are implemented according to their guidelines.

Before a Governance internal audit is conducted, it is essential for the Head of Internal Audit to hold an appropriate position within the organisation, with no impediments or restrictions on information, and for him to have strong support from an Audit Committee.

The aspects to be assessed by the Head of Internal Audit are:

The proper structure and operation of the governing bodies, their diversity, transparency, hierarchical lines and allocation of responsibilities, as well as an optimum combination of specialised knowledge, skills and experience. In this regard, the regulator requires a 'Governance Map' to be produced and maintained.

IIA Standard 2110 is entirely dedicated to the role of governance and the associated 2110 Implementation Guidelines believe it is necessary to speak with other people in key governance positions within the organisation as this can clarify the knowledge held by the Head of Internal Audit on the specific processes at the organisation and the guarantee activities already in place. These key positions include the Chairman of the Board (or elected superior or appointed official at a government body), the Chief Ethics Officer, Chief HR Officer, external auditor and Chief Risk Officer.

In the case of listed companies, auditing the entire Shareholders' Meeting process is enormously important because it is the first link in the chain of governance.

Code of Ethics that the Board of Directors should have, as well as a code of conduct that contains all obligations.

One aspect that should be monitored permanently involves the policies aimed at avoiding conflicts of interest, as well as programmes for detecting the use of privileged information.

Supervising governance responsibility in terms of offences committed by executives/senior management and providing effective reporting channels.

Strategic Plan in order to be properly aligned with the business, knowing the company's policy on new markets, products and services.

IT governance in line with the business targets, data quality management, security and whether that information flows towards the board members to support effective decision-making.

Supervise performance by members of the management body and the various committees in the exercise of their management roles, for which they must be assessed (at least once a year).

Remuneration Policies will need to be revised regularly in terms of design and suitability, as well as the proper function of the Remunerations Committee, which will be responsible for setting the remuneration paid to the management body.

The Succession Plan is an important issue, given that planning the replacement of members of the board of directors generates confidence among shareholders.

This plan demonstrates company readiness to tackle unforeseen circumstances and its ability to maintain the business model under constant review.

Assessment of the Risks, Control and Compliance Department should take place effectively and in a coordinated fashion, via an assurance map wherever possible.

Internal Auditing stands as an essential function for assessing corporate governance and everything possible should be done to intensify its programmes towards the most decisive area of the organisation.

The Succession Plan is an important issue, given that planning the replacement of members of the board of directors generates confidence among shareholders

TOPIC 03

CORPORATE CULTURE

Organisational culture has become an issue of considerable strategic importance. Previously considered as an intangible concept, many organisations now manage indicators on talent, reputation, quality of service and even company revenue linked to corporate culture. When managed well, it can become a strength that sets any organisation apart from its competitors.

HOWEVER, accurately assessing the culture of an organisation is no simple task.

The first reason for this is that the complex structures that exist within many organisations mean that often more than one culture can coexist within an organisation at the same time. This characteristic is common at organisations that have grown through a process of acquisitions.

Furthermore, corporate culture is an intangible concept and therefore difficult to measure and objectify. Individuals perceive the culture of an organisation according to what they see or hear within it and that is why corporate culture is only interpreted through values and conduct.

An outstanding leader can usually be found behind a strong organisational culture (this is often the founder themselves). They tend to be decisive and good communicators, capable of conveying their own personal values and extending them to the organisation as a whole. This distinguishing feature generally provides an advantage when the origins of the conduct transmitted to the organisation is known, but presents numerous drawbacks if the values are not as expected.

Dimensions of corporate culture

Gómez L. and Belkin D. suggest the existence of seven dimensions that, in combination, capture the essence of the culture of an organisation. These dimensions have been described as follows:

Innovation and acceptance of risks: The degree to which employees are encouraged to be innovative and take risks.

Attention to detail: The degree to which employees are expected to demonstrate precision, analysis and attention to detail.

Focus on results: The degree to which managers focus their attention on results and effects, rather than the techniques and processes by which those results were obtained.

Focus on people: The degree to which administrative decisions are taken while considering the effect of the results on the people who form the organisation.

Focus on the team: The degree to which the work activities are organised around teams, rather than individuals.

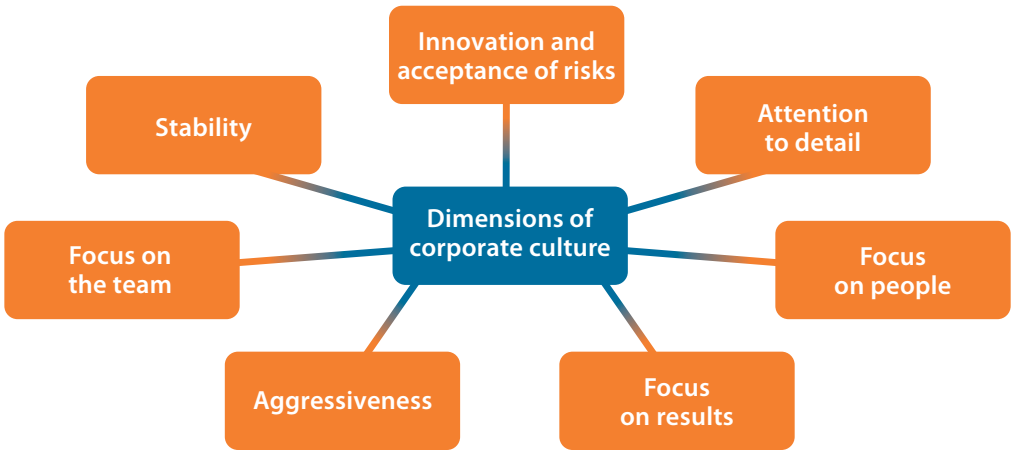
Aggressiveness: The degree to which the people are aggressive and competitive, rather than accessible and obliging.

Stability: The degree to which activity by the organisation places an emphasis on maintaining the status quo.

The acceptance of risk is an important component of an organisation's culture. Some organisations stand out for being highly aggressive, with a very high risk appetite and where the internal auditor does not feel especially comfortable. On the other hand, other organisations eventually disappear because they are incapable of adapting to changes.

Such is the case of companies like Kodak, which was not able to reinvent itself and was made bankrupt by digital technology.

The culture at an organisation can allow certain conduct or inhibit others, leading to a specific way of behaviour



The greatest influence is not always had by the highest ranking employees in many organisational cultures

The Kodak culture was to avoid decisions that implied any kind of risk, but they failed to consider the risk of not changing in an evolving environment.

The culture at an organisation can allow certain conduct or inhibit others, leading to a specific way of behaviour.

Until a few years ago, culture risk was neither considered as something to be supervised nor something that required control mechanisms. However, as is the case with other types of risk, it began to be managed more formally within the financial industry and was promoted by the regulator.

For example, this has been done by the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA), which have published a series of final standards that confirm a focus towards improving individual responsibility in the banking sector. These standards cover the regime for senior executives, the regime for certification and the new rules of conduct.

In June 2013, the Parliamentary Commission on Banking Standards (PCBS) published its report entitled *Changing Banking for Good,* which establishes recommendations for legislative action and other actions to improve professional standards and the culture in the banking sector of the United Kingdom. In the near future (7 March 2017 to be precise) the new Rules of Conduct will apply to all employees of the banking sector.

With measures such as these, regulators seek to enhance one of the most important aspects of a good organisational culture: Ethics.

Internal Audit and Corporate Culture

Whenever the Head of Internal Audit conducts an audit on the organisational culture, he must decide which aspects are valued by all stakeholders and whether the culture is suitable and helps achieve the organisation's objectives.

When weaknesses are identified, he should advise management on how to redefine certain issues while being aware that the results of a firmly rooted culture do not usually take immediate effect.

Furthermore, care should be taken when conveying this to other employees and the impact that these actions may have on the culture should be assessed.

For example, Carly Fiorina failed as CEO of Hewlett-Packard because she tried to impose a sales-focused culture on an organisation led by engineers.

Generally speaking, action plans should be developed from a top-down approach because management should be the first to set an example and reinforce the message defining the desired conduct.

The Institute for Business Ethics has produced the document *Checking culture: a new role of internal audit.*[5.1] According to this document, internal auditors cannot and should not work alone. The Head of Internal Audit can receive valuable as-

sistance and support from others within the organisation, such as the compliance and ethics officers or the human resources officers.

The greatest influence is not always had by the highest ranking employees in many organisational cultures, meaning that it might be important to identify which professionals hold the most sway over their colleagues through natural leadership.

Furthermore, the Head of Internal Audit should consider that the result of any action will most likely not be immediate, meaning that he will need to continuously monitor the changes that take place and ensure that the effects are as desired.

It should be stressed that the Head of Internal Audit should also assess the culture of their own department; their leadership; their way of communicating; and how they are perceived as key issues.

Many organisations obtain feedback through surveys, in which various aspects of the organisation's culture are assessed. This includes, more specifically, the internal audit function.

The 2016 report Organisational Culture, evolving approaches to embedding and assurance, published by the Chartered Institute of Internal Auditors, highlights the complexity of conducting this type of audit and the preparation they require, both by the internal auditor and the Audit Committee itself.

The characteristics of these reviews are not the same as those of a standard audit, except for the reviews related to procedures, policies and processes, and "grey areas" will arise due to the different criteria that will need to be suitably agreed upon.

The greatest influence is not always had by the highest ranking employee in many organisational cultures

TOPIC 04

COMPLIANCE

The role of Compliance has expanded enormously at most organisations due to the effect of globalisation and international growth. In France, for example, Internal Compliance and Control Managers are among the top seven most in-demand jobs.[6]

This process has been boosted in recent years by a number of scandals across the globe, often leading regulators to intervene in order to protect stakeholders and the public interest, in turn contributing to an increasingly complex multi-national legislative environment.

THE NEW named the **General Data Protection Regulation (GDPR)** (Regulation (EU) 2016/679), which will enter into force in May 2018, states that companies that provide services to European Union citizens could face fines of up to 20 million euros or 4% of their global turnover (whichever is highest of the two) if they do not adequately protect and manage data.

On 19 August 2016, the New York Financial Services Department ordered Mega International Commercial Bank of Taiwan to pay a fine of 180 million dollars and instate an independent supervisor after violating the anti-money laundering laws of New York. [7]

The fine was part of a consent order signed with the New York department in which the bank agreed to adopt immediate measures to correct noncompliance, including the hiring of an independent supervisor to deal with serious shortcomings within the bank's compliance programme, and to implement controls against effective money laundering.

Hence, liabilities have been stepped up and may even be of a criminal nature for the legal entity itself. Noncompliance may lead to closure of the company and not only be limited locally but may even affect the parent company, which could involve incalculable reputational damage.

In the United Kingdom, for example, an individual who has committed an offence against the **Bribery Act** might potentially go to prison for up to 10 years and/or pay an unlimited fine, the latter for companies found guilty of such an offence.

In the United States, offences committed under the Foreign Corrupt Practices Act of 1977 (FCPA), can lead to individuals receiving fines of up to 250,000 dollars when found in breach of the law as well as a possible prison sentence of up to five years. A company found guilty under the FCPA is liable for a fine of up to two million dollars.

In Spain, Constitutional Law 5/10, of 22 June, was approved in 2010 (subsequently reformed by Constitutional Law 1/2015), which introduced the concept of **criminal liability** for legal entities into the legal system. **'Due control'** has become an issue since then, as has the need to implement compliance programmes to create **control mechanisms that act as grounds for exemption.**

In certain sectors, such as banking and insurance, this function is already highly developed due to demands from the regulator.

The field of compliance should be in alignment with the corporate governance model of the organisation and have adequate mechanisms for separating powers, responsibilities and decision-making processes.

Furthermore, it should have the necessary support from management, as well as advanced technological resources and professionals with specific skills for effectively performing their role.

COMPLIANCE CULTURE

Many regulators are currently working to change the compliance culture at companies, as well as to legislate on the new corporate models that are arising through new technologies. It is not simply about complying for the sake of complying.

Regulators lack the resources required to exhaustively supervise all organisations. Therefore, a different approach is being sought after, focusing on self-regulation, implementing a corporate culture of integrity, and employing ethical programmes that offer sufficient confidence to all.

In spite of the efforts made, the "ethical blindness" effect - a concept coined by **Professor Guido Palazzo** (the commercial priorities of an organisation push towards bribery and corruption among employees) - will not disappear.

It is no surprise that an increasing number of organisations are making an effort to raise their global corporate governance standards and are dedicating more resources to the development of **whistle-**

The field of compliance should be in alignment with the corporate governance model of the organisation and have adequate mechanisms for separating powers, responsibilities and decision-making processes.

The most important objective of compliance is for an organisation to operate with integrity

blowing programmes. These programmes enable companies to detect and correct internal deficiencies before they become known by the public, thus protecting the value of the interested parties.

There are also programmes that establish rewards for informants who collaborate with the authorities on resolving fraud cases.

On 31 August 2016, the US SEC (Securities and Exchange Commission) announced the pay-out of over 22 million dollars to an informant whose information and extensive detailed assistance helped the agency stop hidden fraud taking place at the company where he worked. This reward is the second-highest amount paid out by the SEC to an informant. The highest figure, amounting to 30 million dollars, was paid out in 2014.

These rewards highlight the importance given by the regulator to reporting channels.

The **FCA** (Financial Conduct Authority) in the UK has also given great importance to the whistle-blower and, since 2015, has published new rules that strengthen this position. [8]

The most important objective of compliance is for an organisation to operate with integrity.

Its role is not only to protect the organisation and its reputation but also to defend the interests of customers, suppliers, partners and anyone else with ties to the organisation.

STRATEGIC ADVISOR

A few years ago, the growth model of an organisation consisted of replicating the same roles as its central headquarters in each country. However, regulatory

inconsistencies between countries mean this is no longer the case.

For this reason, the **Chief Compliance Officer (CCO)** is acquiring an important role as strategic advisor to the business.

In its study entitled ***Local Compliance in Global Business***. A journey through a changing landscape, **BDO** analyses the different organisational models for local compliance adopted by companies and the challenges they face to streamline their processes and guarantee compliance with local regulations.

The outsourcing of roles is usually limited in these cases to the verification of compliance with existing regulations in each country by a local provider. Nonetheless, it can be seen that there is no adequate correlation between the risks stemming from local compliance and the measures adopted by companies to guarantee both the necessary control and visibility at the central headquarters.

Furthermore, the trend is to relocate various process to geographic areas (such as India or China), which enable costs to be reduced substantially or even for the service to be outsourced.

The completion of **Due Diligence** tasks by these service providers takes on extraordinary importance given that the regulatory risk is not conveyed.

It is also important to state that most regulatory risks are transversal (the regulator is focusing on areas of governance, risk management, data protection, cybersecurity, etc.) -meaning that they affect various departments- and this means that correct **coordination** between the various oversight areas becomes necessary.

This adaptation by the organisation to regulatory requirements - where certain processes sometimes need to be changed or new ones implemented - will be an opportunity for the Head of Internal Audit to actively participate as an Advisor.

It can be seen that there is no adequate correlation between the risks stemming from local compliance and the measures adopted by companies

TOPIC 05

WORKING ENVIRONMENT

The working environment is a hugely important factor at almost every organisation nowadays. A good working environment tends to usually be associated with productivity, and this becomes a competitive advantage in an increasingly complex environment.
The image projected by organisations to the public is also a concern; in the modern era breaches in professional standards can potentially be transmitted and discussed instantaneously via social media networks, something that can either make or break a brand.

Since the early 1960s, organisational behaviour studies have been highlighting how difficult it is to find universal principles for handling different people with different work styles.

The working environment is a tough factor to measure, although it can be diagnosed via anonymous surveys or interviews with staff as they leave the company in order to obtain a real idea of employee perceptions. However, these KPIs are rarely included in a dashboard and rarely given to the audit committee for analysis on a regular basis.

It should be recognised that deterioration of the working environment is a significant organisational risk, which should be handled effectively because it usually leads to other serious issues.

The negative consequences include a failure to adapt by individuals, high staff

turnover, absenteeism, poor innovation, low productivity and unethical conduct.

Workplace stress – such as long hours, job insecurity and lack of work-life balance – contributes in the US to at least 120,000 deaths each year and accounts for up to $190 billion in healthcare costs, according to research by two Stanford professors and a former Stanford doctoral student now at Harvard Business School.

The Head of Internal Audit has incorporated all these factors into the HR Department review that manages this risk, but it is important for this factor to always be considered as an indirect factor during the review of any department.

Our reviews should always consider staff conduct and the way in which they interact with Internal Audit and the customer.

The coexistence within the organisation of different generations (Hot Topic) requires a far-reaching change in team management.

Teams are no longer just multidisciplinary in terms of knowledge levels, but should also be formed by a generational mix that combines experience with talent and can play a key role in creating a suitable working environment.

One way to provide a first impression of the working environment is to review workstations, decoration, out-of-work activities offered, conversation tone and conduct in the cafeteria. These informal aspects may not seem appropriate for analysis by Internal Audit but are highly effective and can provide some important early warning signs.

Furthermore, deterioration in the working environment also directly affects the Head of Internal Audit in terms of managing the internal audit team.

It could be said that the Internal Audit Department is susceptible to various factors:

- It requires significant intellectual effort due to the complexity and variety of the tasks to be audited, as well as ongoing training so as to remain suitably up-to-date.

- Most tasks usually have very strict deadlines that require constant effort to be maintained, travel can be frequent and negotiations with management on recommendations can be tense.

- If a lack of knowledge from the rest of the organisation is added to these ingredients, a deterioration of the working environment is guaranteed.

The Head of Internal Audit is ultimately responsible in internal auditing for creating a pleasant working environment that avoids or minimises stress and leads to the highest level of commitment from members of the department.

Leadership by the Head of Internal Audit

Good leadership that treats each team member as a person and does not merely

Teams are no longer just multidisciplinary in terms of knowledge levels, but should also be formed by a generational mix that combines experience with talent and can play a key role in creating a suitable working environment

The Head of Internal Audit should not be concerned with training his team to do their job right from a technical point of view but rather with qualitative aspects such as security and confidence, which will enhance the working environment

consider them as a resource is essential for success.

Employees should feel **involved in goals and assume organisational principles or values as their own,** thus incentivizing the desired conduct. To do so, the Head of Internal Audit should be an expert communicator who knows how to transmit these values and targets and is capable of creating an environment in which all members of the department - regardless of their category - feel important.

The Head of Internal Audit should not be concerned with training his or her team to do their job correctly from a technical point of view, but rather focus on qualitative aspects such as security and confidence – matters that could enhance the working environment.

They should be able to recognise and identify the relevant personal issues of interest to each employee, for which heads of internal audit need a good level of emotional intelligence and an ability to foster commitment and look after talent.

The HIA should create a bond of friendship and trust through personal meetings (or online meetings when different geographical locations are involved), breakfasts, or any other activity that facilitates direct knowledge of the employees' expectations.

Furthermore, recognition of a job well done is always an important motivational factor. Positive reinforcement should play a major role in this, but the Head of Internal Audit demonstrating themselves to be a committed individual ready to help whenever necessary can also be highly beneficial.

The Head of Internal Audit will interact with the next generation (Hot Topic) of internal auditors, whose mentality can often differs from that of older generations and who demonstrate great talent and charisma while demanding substantial changes in terms of work.

Such aspects as increased working hour flexibility, teleworking or target-based working are components that will lead to departmental transformation.

Reducing bureaucratic issues, improving processes and streamlining them as far as possible, as well as working towards improved supervision, will help improve the working environment.

The Head of Internal Audit should be a professional who can **inspire passion** and ensure that internal audit teams **innovate** and improve to create value in the department while tolerating failure, mistakes or the consumption of time with limited results.

TOPIC 06

MANAGING THE NEXT GENERATION

It is estimated that 27% of the world's population (two billion people) belong to the so-called Generation Y or "Millennials" (19-35 years old) and another 32% (2.4 billion) belong to the following generation, known as Generation Z or "Centennials" (0-18 years old). In total, they account for 59% of the global population and in 2020 they will make up 60% of the workforce.

These two generations are the most numerous in history and possibly the most different from their predecessors, with characteristics that are leading to unprecedented changes at organisations everywhere.

They are both characterised by an embrace of diversity, sustainability and globalisation. They have grown up in the era of cutting-edge technology and its everyday application to their daily lives. According to the World Economic Forum 2016, 86% of "Millennials" have a favourable attitude towards technology and believe it is creating jobs rather than destroying them.

They are therefore open to creating new business models such as those launched by benchmark figures -teenage businessmen that include Mark Zuckerberg, Wang Xinwen, Tavi Gevinson, Elon Musk, Robert Nayo and Maddie Robinson, among others- who became multimillionaires doing something they liked and believed in.

If an organisation is incapable of offering an immediate response, it runs the risk of losing the customer

Approximately 55% of 10,000 young people from Generation Z surveyed by Universum are interested in setting up their own business, with this figure rising to 75% of those surveyed in such regions as the Middle East, Central Europe and Eastern Europe. The greatest goals are to become one's own boss and have an impact on society.

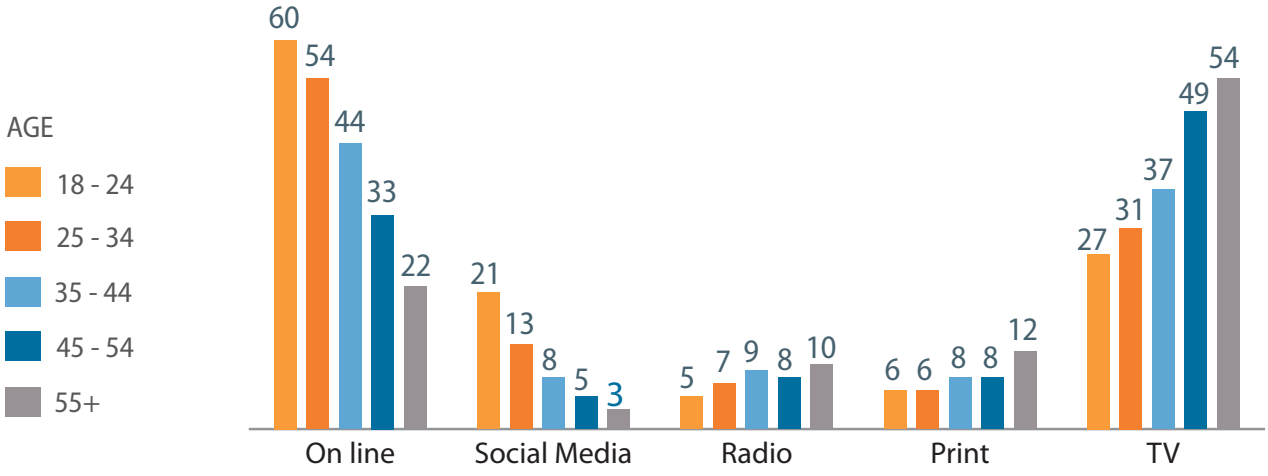
As workers, they are non-conformist professionals who demand employment flexibility and value quality of life over and above their professional career. At the same time, they are highly pro-active, have the energy to propose change and are not afraid of presenting innovative ideas.

However, as stated by Rick Goings, Chairman / CEO of Tupperware Brands, "Millennials want to have their own businesses but, when you look at their skillsets, many of them possess cognitive skills yet lack such non-cognitive skills as leadership, interpersonal skills and the concept of teamwork".

In contrast, both generations like to maintain relations via smartphones, apps and social media networks and, as customers, they are demanding that companies interact with them in the same way. For example, Facebook claims that "Millennials" check their mobile telephones about 150 times a day, compared with the 30 times a day for all other adults.

They are information-focused (60% of the youngest "Millennials" around the world (18-24 years old) use the Internet as their main source of news) but, unlike previous generations, they do not access this information via the TV or the printed press. Furthermore, they compare information from various sources and in turn disseminate this information themselves through social media.

Main sources of news by demographic cohort



Source: University of Oxford, Reuters Institute

The effect of these generations on most organisations due to the way they interact and their critical behaviour is undeniable.

These new ways to communicate have entirely revolutionised the advertising sector, because these generations like to express opinions within seconds about any product purchased or the service they received via such online platforms as Yelp, websites and forums or blogs, on which they share their purchase experience with thousands of potential customers.

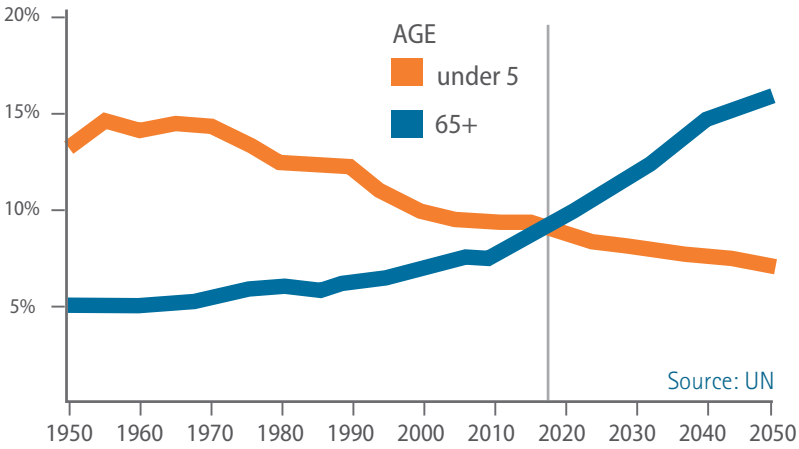
Their opinions are so important that Barkley Advertising Agency states that 68% of "Millennials" do not take a decision without first discussing it with others and approximately 51% trust "strangers" even more than their friends when planning a significant purchase.

By being born and raised in the era of technological development and the Internet, they are used to instantaneous communication and are therefore impatient. Hence, if an organisation is incapable of offering an immediate response, it runs the risk of losing the customer.

"In real time" has become real: "There are big implications for brands when we think about connecting with an audience that claims they can respond to 40 snaps in a minute". [9]

These generations value response speed over formality as they use casual language and include such things as "emojis" in their mobile communication - used by up to 90% of "Millennials" according to the Bank of America's Consumer Mobility Report 2016. It is used so much and has become so greatly ingrained on the youth consciousness that the "Word of the Year 2015" from the Oxford Dictionary was an emoji ("Face with Tears of Joy").

Number of 65+ will overtake those aged <5 by the end of this decade



New Challenges and Implications

Both the "Millennials" and the "Centennials" face a significant challenge from a demographic point of view due to a falling birth rate and rising life expectancy. In 2020, for the first time ever, the number of people over the age of 65 will be higher than the number of children aged 5 or less. In 2050, the "Silver" Generation (65 years old and above) will have increased from 885 million people to 3.4 billion. [10]

These problems could mean that Generations Y and Z will end up being poorer than their parents and grandparents, with the corresponding problem for economic growth and creating a future

Creating a future scenario in which we will be forced to seek solutions to the problems affecting health, housing, pensions, labour markets, public finances and other types of risks that will transform the economy as we know it today

scenario in which we will be forced to seek solutions to the problems affecting health, housing, pensions, labour markets, public finances and other types of risks that will transform the economy as we know it today.

For this reason, organisations that fail to consider this reality will face serious problems. Nowadays, HR managers are highly conscious of this transformation and are working hard to manage the special features of these professionals.

They will also need to strengthen other aspects related to the soft skills that have been gradually lost and are indeed important

The Role of Internal Audit

These changes at organisations also affect Internal Audit, requiring the Head of Internal Audit to check the measures being adopted by the organisation to adapt its image, to develop new products and services aimed at younger generations, and to incorporate a new way of interacting with them. They are also being required to properly manage their teams and, as stated by the study entitled The Millennial Auditor (Source: Wolters Kluwer), harness the skills of these new generations with new technologies and their relationship with the environment.

On the other hand, they will also need to strengthen other aspects related to the soft skills that have been gradually lost and are indeed important, such as interview skills, the ability to communicate via the written form effectively, and drawing up an internal audit report. Furthermore, in order to retain the talent that these generations possess, efforts should be made to strengthen the working environment (Hot Topic).

TOPIC 07

CYBER-SECURITY

Cyber-security has become one of the priority risks to be dealt with by organisations given that the number of cyber-attacks is on the rise every day; they are increasingly sophisticated and have an enormous economic and reputational impact on organisations.
Governments are not immune to this threat. For example, Chinese hackers alone have caused damage valued at over 100 million dollars to the US Defence Department's networks according to documents leaked by Edward Snowden.

In 2012, this same department was suffering over 10 million cyber-attacks per day. Given the rapid development of cyber-criminals, it would be reasonable to assume that this figure has risen drastically since then. The US Marine Corp is another example, which receives 110,000 cyber-attacks every hour.

Even the most heavily protected organisations suffer from cyber-attacks and the theft of all sorts of data (dataleaks), leading to corresponding and enormous economic and reputational losses. Industrial espionage is among the objectives sought by these cyber-criminals.

For example, the 20 largest cyber-attacks carried out in France in 2015 were linked to this objective [11]; and, in 2014, a cyber-attack against JPMorgan Chase jeopardised the accounts of 76 million households and 7 million small businesses, with results that dwarfed the

On 6 July 2016, the European Parliament approved the first European Directive on cyber-security - The Directive on Security of Network and Information Systems (the NIS Directive)

preliminary estimates made by the bank and made this attack one of the largest intrusions every carried out.

The Threat Landscape 2015 (ETL 2015) drawn up by ENISA (European Union Agency for Network and Information Security) is the result of an analysis of information threats in Europe revealed between December 2014 and December 2015, and provides an analysis of the situation and the cyber-threat environment dynamic. [12]

Data Protection, the workhorse for organisations

Data protection gains particular significance against this backdrop, not only for meeting the new EU Regulation but because the opening up of new communication channels has led to a highly significant increase in fraud (especially the risk stemming from impersonation).

Most banking services have stepped up online transaction security by using Two Factor Authentication technologies (2FA), which verify identity twice. This type of technique requires users to provide some other identification besides the usual password to corroborate that the person really is who they say they are.

On 6 July 2016, the European Parliament approved the first European Directive on cyber-security - **the Directive on Security of Network and Information Systems** (the NIS Directive) - in order for companies that provide essential services to improve their defence capabilities against cyber-attacks and to report incidents to the national authorities.

We have learned a great deal since MyDoom (the most expensive virus in the world in the history of cyber-security, which caused financial damages estimated at 38.5 million dollars), was discovered for the first time in 2004 and became the fastest-spreading email worm ever known. This incident made organisations realise the importance of having modern protection software (anti-malware programs) on all devices.

But an antivirus is not the only protection we should equip ourselves with. Let us not forget that cyber-criminals also use many other techniques, such as social engineering and phishing.

In the context of information security, **social engineering** refers to the psychological manipulation of people to perform certain actions or reveal confidential information. It is a type of scam aimed at gathering information, fraud or access to a system using such techniques as like-jacking, link hacking, phishing, spam, etc.

For example, a big international cyber-criminal network based in Eastern Europe managed to steal a billion dollars over two years in an attack on 100 different banks in almost 30 countries using phishing emails targeted at bank employees [13]

People are the weakest link when it comes to cyber-security and the reason

why the psychological manipulation of cyber-attack victims is so common.

Users who spend a lot of time on social media networks are highly susceptible to clicking on links published by trusted friends, which information pirates use to their own benefit.

These are just some of the most popular cyber-attacks targeted at social media platforms.

Training Internal Audit Departments in IT is essential

Cyber-security is something that all organisations are already fully aware of and it should therefore form an important part of the internal audit plan of any Internal Audit department. Assessing the effectiveness of cyber-security requires highly specialised professionals and the Head of Internal Audit should therefore make sure they have the right individuals on their team. It is standard practice to outsource part of these checks due to the difficult nature of the task and the complexity involved in staying up-to-date.

The Head of Internal Audit should regularly assess the corporate information security policies, their sturdiness and the awareness of them among employees.

All members of the organisation need to be trained but a special focus should be placed on executives given the importance of the sensitive data to which they have access.

Cyber-security should be included as a routine part employees' daily working lives (Internet security at home, USB encryption, use of antivirus programs, file download or browsing certain pages, among other things) in order to avoid malware.

IIA Standard 1210.A3 states that internal auditors must have sufficient knowledge of key information technology risks and controls and available technology-based audit techniques to perform their assigned work. However, not all internal auditors are expected to have the expertise of an internal auditor whose primary responsibility is information technology auditing.

The Head of Internal Audit should be aware of internal software developments that are taking place at their organisation, checking that they have the proper security measures before entering production and performing ongoing audits given that these are ever-changing systems.

In this regard, the document entitled *Cyber-security, a Global Challenge* by the Bankinter Innovation Foundation states that metrics are necessary for determining and establishing objectives aimed at genuinely knowing whether a piece of software is truly good or not, as well as the level of security it offers. However, it is difficult to determine a point of reference for marking a limit between secure and insecure in the field of software.

The Head of Internal Audit should also assess the action protocols in the event of an attack, ensuring they remain up-to-date and maintaining company resilience

All members of the organisation need to be trained but a special focus should be placed on executives given the importance of the sensitive data to which they have access

(the ability to absorb adverse internal and external impacts and recover with a view to returning to normal operations in a controlled fashion).

In 2014, the **National Institute of Standards and Technology** (NIST) developed a control framework that could be highly useful to use when facing these risks, even though additional assessments may be required under **ISO 27001 and 27002** to allow for greater guarantees. This framework contains a series of best practices and includes a methodology for protecting individual privacy, and provides guidelines on cyber-security activities and risks by considering them as just another part of the organisation's risk management processes.

The IIA's newest **Global Technology Audit Guide, Assessing Cybersecurity Risk: Roles of the Three Lines of Defense** offers guidance to internal auditors on how to update their approach to provide assurance over cybersecurity risks. It also empowers Head of Internal Audit to put forth a clear audit approach to assess cybersecurity risk and management's response capabilities, with a focus on shortening response time. [14]

Not all cyber-security risks stem from the Internet but rather require physical measures that we should also be aware of, such as access protection for the office or other sensitive areas

In spite of the above, not all cyber-security risks stem from the Internet but rather require physical measures that we should also be aware of, such as access protection for the office or other sensitive areas.

Service outsourcing is not exempt from this supervision. Service providers that have access to part of the company's information should have similar or higher security levels to those held by the organisation and we should duly monitor their activity.

TOPIC 08

FRAUD & CORRUPTION

Fraud remains one of the main concerns for the internal auditor as it affects organisations of all sizes, generating a significant direct impact on organisations' bottom lines and damaging corporate culture.
The "2015 Kroll Global Fraud" survey conducted by Kroll - a consultancy firm that specialises in the management of business intelligence and information - of 768 executives from various industries around the world found that 75% of the companies surveyed claim to have been the victim of fraud within the last 12 months. In addition, 81% of companies recognise internal factors as the source of this fraud.
Technological fraud has experienced the fastest growth in recent years, becoming increasingly sophisticated. The 2016 Global Fraud Study by ACFE estimated that the typical organisation loses 5% of revenue in a given year as a result of fraud.

HOWEVER, FRAUD ALSO LEADS to a loss of customer confidence, meaning that the indirect impact caused by a worsening image for the organisation is difficult to quantify.

This pressure is compounded by that exerted by regulators, which demands an effective protection framework for extenuating administrative or even criminal penalties.

Regulators ensure that organisations create assurance structures to mitigate bribery and corruption, money laundering and accounting fraud, but these systems are not infallible. In 40.7% of cases, the victim organisation decided not to refer their fraud cases to law enforcement, with fear of bad publicity being the most-cited reason (Source: ACFE).

Wherever fraud is being fought, it is important to establish how management attempts to convey an environment of ethical and socially responsible conduct.

At the top-end of the organisation, the Head of Internal Audit should focus on identifying Bribery and Corruption issues (ISO 37001), which represent a major risk for the organisation

The Head of Internal Audit should ensure that these internal controls are adequate and should assess weak spots that could allow fraud to take place, not merely strengthening controls but proposing changes to processes that would eliminate the opportunity.

At the top-end of the organisation, the Head of Internal Audit should focus on identifying Bribery and Corruption issues (ISO 37001), which represent a major risk for the organisation, while focusing on asset misappropriation in other areas of the organisational structure, which generally have a lesser impact.

There is no doubt that organisations should continue investing in detection programmes that enable the most common red flags to be identified and strengthening preventive programmes, because they are always the most effective.

Developing an anti-fraud programme and establishing an ethical culture within the organisation and vis-a-vis third parties related to company activity is the best deterrent.

This programme should establish "zero" tolerance to all kinds of fraudulent behaviour, regardless of the amounts involved and at whatever level of the organisation.

But, how can we detect fraud? We should recognise that most cases of fraud are revealed by chance or reported, and the worrying fact (it affects our reputation as a profession) is that a considerable amount of time has usually passed without any control or oversight activity having detected it.

The first action that the Head of Internal Audit should take is to analyse the Hot Line (whistle-blowing programme), an essential tool that should be reinforced.

For this tool to be effective, it should offer a swift response to the whistle-blower, guaranteeing their protection and decisive action in those cases where the report is found to be true.

Employees will only use this channel if they fully trust it and see that it works with no consequences for the whistle-blower. Furthermore, this tool helps detect internal control problems that could affect the criminal risk prevention plan, offering a swift solution to the problem and revising said plan.

Fraud-related tasks require very specific skills from the internal auditor, and ongoing training on both the types of fraud that exist and the corresponding detection techniques should be a priority for all internal audit departments. Internal auditors do not need to be fraud experts but, as stated by Standard (1210.A2), they should have sufficient knowledge so as to assess the fraud risk and the way in which it is managed by the organisation.

In September 2016, COSO published a Fraud Risk Management Guide, intended to be supportive of and consistent with the 2013 Framework and serving as a best practice guidance for organizations to follow in addressing this new fraud risk assessment principle.. [15]

Whenever we undertake this type of task, we should work under the premise that all our evidence could be used in court,

meaning that we should act with due professional care so as not to invalidate any possible future evidence.

The technological resources available organisations are outstanding tools for fraud detection. Internal audit should harness the potential of big data to identify patterns and atypical behaviour for further investigation. For over a decade, we have also had an ally that facilitates our work and is constantly improving: Artificial Intelligence, something used by pioneers in fraud prevention in sectors such sectors as telecommunications, insurance, and banking.

There are various techniques for combating fraud with artificial intelligence, such as supervised neural networks and diffuse neural networks, which are particularly used in the world of finance to avoid both telephone fraud and credit/debit card scams.

Hidden Markov models or Bayesian networks are also common ways to identify patterns, in which probabilities are established and uncertainty over whether fraud was involved in specific conduct is reduced.

The task would be made easier if the patterns coincided with the transaction records, but fraud changes constantly and this makes it difficult to detect when committed for the first time.

The advantage of Bayesian networks is that they have a much shorter learning period than neural networks, while neural networks assess new examples faster. The following document offers a good practical example: Credit Card Fraud Detection Using Advanced Combination Heuristic and Bayes' Theorem. [16]

For the time being, the best way to combat fraud is by using "Augmented Intelligence" - a relatively new concept - The essence of "augmented intelligence" is the unification of the best human skills with the best advantages of machines. [17]

At present, all fraud detection techniques continue to advance and the cost/benefit ratio of detection continues to fall due to a lower number of false positives (Source: Data Mining Techniques in Fraud Detection). [18]

The largest company owned by the Community of Madrid - Canal de Isabel II Gestión, which is responsible for the integrated water cycle in the Region of Madrid - decided in 2014 to purchase high-resolution images from the French space agency CNES, which has its Pleiades satellites in orbit and capable of taking photographs of any part of the world in extremely high definition.

After examining 120,000 swimming pools and 23,000 hectares of parkland, meadows and gardens, the Research, Development and Innovation Department of Canal de Isabel II discovered a 10% "inconsistency" in water consumption, which was then analysed by its Fraud Division to reveal liabilities.

Management should be aware that more controls imply less fraud but, combined with Integrated Thinking and oversight of corporate culture (Hot Topic) are also essential deterrents that should be developed by the Head of Internal Audit.

Internal auditors do not need to be fraud experts but, as stated by Standard (1210.A2), they should have sufficient knowledge

TOPIC 09

TRUSTED ADVISOR

Confidence within an organisation is essential for the entire corporate structure to function correctly. "Global Generations 3.0" research, released by EY in June showed a survey of nearly 10,000 workers ages 19 to 68 in eight countries revealed that just 46% of employees placed "a great deal of trust" in their employer, and only 49% placed "a great deal of trust" in their manager or colleagues.

THESE DATA SHOW a risk that needs to be minimised because it generates strain on the working environment (Hot Topic). increased staff turnover and unbalanced decision-making.

Over time, management should build trust elements based on transparency, sincerity, ability to admit mistakes and, naturally, by transmitting the corporate ethic not only in words but in actions.

However, in turn, who can senior management trust? Who can senior management consult on important decisions?

The role of the internal auditor as trusted advisor

The Head of Internal Audit should raise his or her profile within the organisation

through the figure of trusted advisor because, by not doing so, there exists the risk of falling out of the loop regarding the organisation's strategy and losing control over the decisions reached, thereby becoming an irrelevant figure that can only act after the damage has already been done.

Heads of Internal Audit should adopt a proactive attitude in this regard because they have the perfect characteristics for performing this task. However, certain significant barriers within the corporate culture must be broken down beforehand.

First of all, it is necessary to gain the confidence of management by demonstrating that they are not only providers of assurance but can also offer other value added services. The Head of Internal Audit should raise awareness of his or her product within the organisation via an internal marketing programme if necessary.

Secondly, they should gain the confidence of management by including executives in the work to draw up the Annual Plan, providing them with information and responding to the work they request. In short, by involving them in the control environment.

It is also essential to have sufficient backing to undertake this work. The Audit Committee itself should support the Head of Internal Audit, and will be decisive in the relationship created between him and the top executives at the organisation.

The Audit Committee should ask the Head of Internal Audit about which activities are being undertaken to achieve this goal at least once a year. The main purpose of a trusted advisor within the organisation will be to help management make decisions.

Participation by the Head of Internal Audit on the Executive Committee will be the ultimate demonstration of trusted advisor status, helping improve understanding of the organisation's strategy plan and development of the business.

The work of the Head of Internal Audit will be to help management make decisions based on knowledge, the use of technology and good data quality, which enable reliable information.

Whenever management debates an issue, it is important to have complete and reliable information. However, the most complicated aspect is that these decisions must often be made within a very short timeframe. Such decision-making processes require various alternatives to be assessed, targets sought and a careful analysis of the consequences that could arise for the business and the organisation's assurance structure.

The Head of Internal Audit will implicitly ensure that no action by management can weaken the internal control structure and should understand that many of the factors that influence the decision-making process are not going to follow the logical process that we expect, meaning that he or she must act as a facilitator in pursuit of solutions and advice, providing understandable conclusions, adapting to any stakeholder

The Head of Internal Audit will implicitly ensure that no action by management can weaken the internal control structure

and demonstrating a sizeable dose of emotional intelligence.

He or she should have the courage and confidence to advise that which others dare not mention and, above all, that which management does not like to hear initially.

The position of Internal Audit within the organisation represents an advantage because it provides the independence required for enabling all sorts of assessments to be made without feeling conditioned by the environment or knowledge of the organisation's structure, internal control status and the risks that provide him or her with a holistic outlook that others do not have.

The polite fiction that occurs in the children's story The Emperor's New Clothes can be reflected in the structures of many companies; i.e. that, blinded by the tricks of a jester and the silence of his court, which dares not contradict him, he walked before his subjects thinking that he was wearing spectacular robes when in fact he was naked. His advisors wanted to avoid conflict by evading confrontation and aligning themselves with the same beliefs as the emperor without trying to find a different argument.

One essential characteristic for being a trusted advisor is to be an excellent communicator who listens to and analyses information in a critical, objective and rational manner without inferences.

One essential characteristic for being a trusted advisor is to be an excellent communicator who listens to and analyses information in a critical, objective and rational manner without inferences

The Head of Internal Audit should consider the subtle details that may pass unnoticed but should not loss the big picture. When making recommendations, these could be considered tools for gaining the confidence of management.

There are recommendations that the recipient does not initially agree with, meaning that the Head of Internal Audit should be capable of persuading others of the advantages to be gained from implementing a certain action plan. The recipient should not perceive this as an instruction or an imposition but rather as a constructive action that incorporates suggestions based on best practices. Knowledge of best practices will be a differentiating factor and recognised by the organisation.

The organisation is no longer content with doing things well but rather wishes to do things better than anyone else and, in such a volatile and complex environment, having a trusted advisor could be something that provides an edge over the competition.

Heads of Internal Audit are trained to perform this difficult role of trusted advisor but should not forget that they are ruled by the Internal Audit standards established by the International Professional Practices Framework, implying the utmost professional care so as not to step over certain red lines that are known to all and analysed in various documents of the IIA Global and the Institute of Internal Auditors of Spain.

TOPIC 10

TRANSFORMATION

Not only is the technological revolution transforming organisations and making them more efficient, it is also bringing disruptive changes to almost every process, especially those that affect relations with customers, suppliers, and even employees.
These new processes represent a significant cultural change, in which the digitalisation of operations, the automation of processes and customer self-management are leading to enormous benefits. At present, processes are almost entirely designed using intuitive software and cater to almost all business processes while generating very few operational errors. Technological fraud has experienced the fastest growth in recent years, becoming increasingly sophisticated.

THIS NEW WAY OF DOING BUSINESS is completely transforming processes, altering risk exposure and leading to an unprecedented internal transformation.

However, organisations have not only changed due to technological advancements. Other changes have arisen because of customers in an attempt by organisations to react to the behaviour of a new generation of consumers, as well as to meet the increasing protection demands from the regulator.

The customer is no longer a passive subject who receives a product or service but rather an employee of the marketing department, thanks to the social media networks, or a data manager responsible for entering, correcting and amending their own data. It could be said that they have been incorporated into the organisation's processes.

The risks tend to increase throughout this adaptation process and, furthermore, the changes that take place usually fracture the internal control structure of the organisation.

The Head of Internal Audit should be highly aware of the entire transformation that

The risks tend to increase throughout this adaptation process and, furthermore, the changes that take place usually fracture the internal control structure of the organisation

may be taking place, because it means exposure by the company to new emerging risks and requires a constant review of the internal control in place at the organisation (what might be working today could stop working tomorrow).

Just as the organisation is changing, Internal Audit is also transforming; and not only because of technological changes.

The role of Internal Audit has gained strength in recent years because stakeholders have chosen this role as being responsible for guaranteeing a reasonable assurance structure within the organisation.

Clearly identifying this responsibility provides satisfaction and highlights the profession in the best possible light. However, it also requires the utmost level of excellence, which will mean that this transformation is sought while considering various factors.

The Head of Internal Audit should use his experience and methodology to assess the design of those apparently "perfect" processes and detect internal control weaknesses in time so they can be corrected.

He should also regularly assess the risks to which the organisation is exposed, placing a focus on governance risks (Hot Topics) but without forgetting other risks that could go unnoticed, such as third party-related risks.

This means that we should audit from top to bottom but also from inside to out, attributing the necessary importance to each activity.

The audit scope is growing ever larger, which creates problems not only when drawing up an internal audit plan but also for the correct implementation of those plans.

Internal Audit departments are being asked to harness this technological environment to review, almost in real time, all the data from a process and identify any anomalous conduct related to fraud and information security or that affects the business.

It would not make much sense for the entire organisation to be transforming itself digitally and the Internal Audit Department lacked the software that would enable it to minimise or eliminate any manual processes.

Internal Audit should be more proactive, moving towards more predictive management, and this transformation should be harnessed so as to switch the focus away from the process, towards the more strategic and decisive aspects for business continuity.

Under pressure from the efficient environment of the organisation, Internal Audit should abandon particularly administrative archaic processes that generate excessive resource consumption, to seek balance in its approach to tackling the internal audit plan.

Many organisations demand more be done with fewer resources and this is usually achieved by changing the focus of our reviews, streamlining the path to a recommendation and maximising the use of the technology at our disposal.

According to Benchmarking Internal Audit Maturity **(The Global Internal Audit Common Body of Knowledge 2015)**, the use of technology is an indicator of internal audit department maturity.

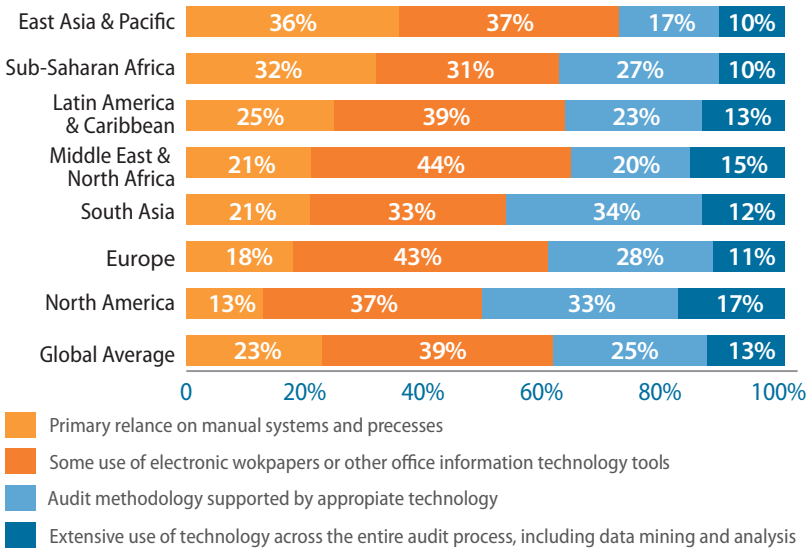
The 39% of the responding HIAs say their internal audit departments are supported by appropriate technology, or they use extensive technology across the entire audit process, including data mining and analysis.

The audit committee should also be aware that this new technological environment implies an increased budget due to investment in both software and hardware, as well as resources allocated to training.

Furthermore, new skills will be needed within audit teams, which will be more multidisciplinary and require multiple supervisors with significant expertise.

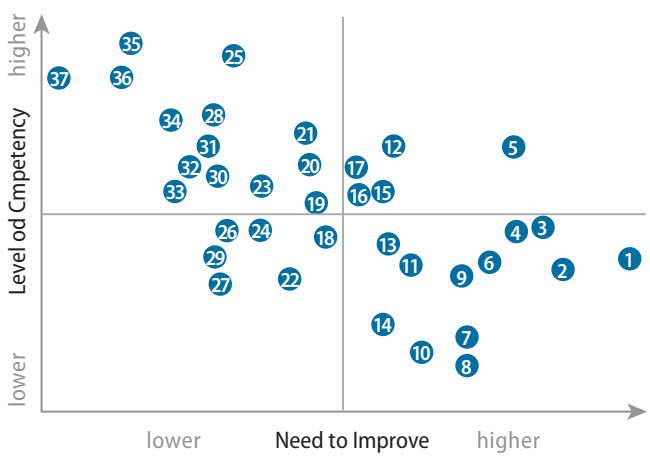
According to the document by Protiviti entitled *Arriving at Internal Audit's Tipping Point.* Amid Business Transformation 2016,[19] the current audit process of knowledge would be established as follows:

Use of technology to support Internal Audit Processes by Global Region



Source: CBOK 2015

Audit Process Knowledge- Perceptual Map



Source: Protiviti

Number	Audit Process Knowledge	Number	Audit Process Knowledge
1	Data analysis tools - statistical analysis	20	Continuous auditing
2	Auditing IT - security	21	Operational auditing - risk based appoach
3	Auditing IT - continuity	22	Auditing IT - computer operations
4	Fraud - fraud detection/investigation	23	Assesing risk - process, location, transaction level
5	Quality Assurance and Improvement Program (IIA Standard 1300) - Ongoing Reviews (IIA Standard 1311)	24	Auditing IT - change control
6	Auditing IT - program development	25	Audit planning - process, location, transaction level
7	Assesing risk - emerging issues	26	Fraud - fraud risk assessment
8	Auditing IT - new technologies	27	Auditing IT - IT governance
9	Marketing internal audit internally	28	Operational auditing - cost effectiveness /cost reduction
10	Computer-assisted autid tools (CAATs)	29	Quality Assurance and Improvement Program (IIA Standard 1300) - Periodic Reviews (IIA Standard 1311)
11	Continuous monitoring	30	Fraud - fraud risk
12	Data analysis tools - sampling	31	Top-down, risk-based approach to assessing internal control over financial reporting
13	Fraud - management/prevention	32	Assessing risk - entity level
14	Data analysis tools - data manipulatioin	33	Self-assessment techniques
15	Operational auditing - efectiveness, efficiency and economy of operations approach	34	Presenting to senior management
16	Quality Assurance and Improvement Program(IIA Standard 1300) - External Assessment (IIA Standard 1312)	35	Audit planning - entity level
17	Fraud - monitoring	36	Report writing
18	Enterprisewide risk management	37	Audit sampling principles
19	Fraud - auditing		

We should audit from top to bottom (top-down) but also from inside out (inside-outside), attributing the necessary importance to each activity

We can see that, in terms of training, there is still a significant gap between the level of competence and the need to improve.

One key factor when transforming the department and increasing its level of maturity is to enhance the use of data through ongoing audits.

The use of data for continuous audits has become essential and there should be no excuse for not implementing distance / continuous audit programmes.

This activity enables internal auditor travel costs to be reduced significantly, as well as any incident to be identified faster, which will enable the appropriate corrective action and create a good sense of control.

Automation of a large part of the process means that the internal auditor can focus on analysing the alerts.

Besides the changes taking place to internal audit processes, the growth of various assurance departments is also important. These departments are growing so fast and their responsibilities are so complex and cross-cutting, that the organisation is demanding coordinated action between them so as to eliminate not only inefficiencies but also assurance voids.

Maintaining an assurance map will be the most effective tool for undertaking this mission and will underpin our role as being most responsible for the proper function of risk controls at the organisation.

The Head of Internal Audit will not only need to make an effort to oversee the proper operation of the entire structure and thus offer absolute confidence to the audit committee but also ensure that everything is operating efficiently, thereby obtaining recognition from management.

SOURCES

1 https://openknowledge.worldbank.org/bitstream/handle/10986/24319/9781464807770.pdf?sequence=6

2 http://www.realinstitutoelcano.org/wps/wcm/connect/22da46004ca35c14a512efb6e29671b7/Global_Presence_2016.pdf?MOD=AJPERES&CACHEID=22da46004ca35c14a512efb6e29671b7

3 https://www.aqmen.ac.uk/sites/default/files/TheViewFromTheContinent_REPORT.pdf

4 Baisse du tourisme en région parisienne #AFP pic.twitter.com/fzbzXz9EIJ— Agence France-Presse (@afpfr) 23 August 2016.

5 https://europa.eu/globalstrategy/sites/globalstrategy/files/about/eugs_review_web_6.pdf

5.1 http://www.ibe.org.uk/list-of-publications/67/47

6 http://abonnes.lemonde.fr/emploi/article/2016/09/13/cadres-quels-ont-ete-les-metiers-les-plus-porteurs-en-2016_4996777_1698637.html

7 http://www.dfs.ny.gov/about/ea/ea160819.pdf

8 https://www.fca.org.uk/news/press-releases/fca-introduces-new-rules-whistleblowing

9 Source: McCann Truth Central 2016

10 Source: United Nations

11 http://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/la-france-a-ete-la-cible-d-une-vingtaine-de-cyberattaques-majeures-en-2015-598189.html

12 https://www.enisa.europa.eu/publications/etl2015

13 Kaspersky

14 https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG-Assessing-Cybersecurity-Risk-Roles-of-the-Three-Lines-of-Defense.aspx

15 http://www.coso.org/documents/COSO-Fraud-Risk-Management-Guide-Executive-Summary.pdf?_ga=1.192669539.870338647.1474276086

16 http://www.ijircce.com/upload/2015/april/13_Credit.pdf

17 http://jolt.richmond.edu/v17i3/article11.pdf

18 http://ojs.jdfsl.org/index.php/jdfsl/article/viewFile/180/108

19 https://www.protiviti.com/sites/default/files/united_states/insights/2016-internal-audit-capabilities-and-needs-survey-protiviti.pdf