SPECIAL EDITION

MADRID EUROPEAN CONFERENCE FOR SUPER INTERNAL AUDITORS

MADRID 3-5 OCTOBER 2018

PUMP UP YOUR POWERS!!
Integral Service, Innovative Approach

Audit, Assurance, Technology Risks & Data Analytics

A team of certified internal auditors who understand your auditable universe

5 continents + 150 countries + 22,500 professionals

Bilbao | Madrid | Donostia-San Sebastian | Palma de Mallorca
Pamplona | Santa Cruz de Tenerife | Sevilla | Valladolid | Vitoria-Gasteiz

Don’t miss the Report on the risks of Cloud Services

www.pkf-attest.es/informe-riesgos-tecologicos
+34 915 56 11 99

Other PKF Attest services: IT Consulting, Financial Advisory, Incentives for R&D, Tax&Legal, Forensic, Corporate Finance
MADRID EUROPEAN CONFERENCE

06 WELLCOME RECEPTION AT SANTIAGO BERNABÉU

08 Ernesto Martínez
OPENING SESSION: PUMPING UP OUR POWERS AS SUPER INTERNAL AUDITORS OPENING ADDRESS

10 Farid Aractingi
THE CHANGING FACE OF THE INTERNAL AUDIT IN EUROPE

12 Josep Piqué
KEYS TO UNDERSTANDING THE GLOBAL GEOPOLITICAL CONTEXT

14 Nassim N. Taleb
THE LOGIC BEHIND RISK-TAKING

16 Andries Terblanche and Juan Mazarredo
THE WORLD IS CHANGING BUT HOW CURRENT INTERNAL AUDIT PRACTICES ARE RESPONDING TO THIS NEW NORM?

20 Alberto Ferreiro
KEY ACTIONS FOR AN EFFECTIVE INTERNAL AUDIT DIGITALIZATION: THE FERROVIAL EXPERIENCE

22 Serenella de Candia
PROVIDING ASSURANCE THROUGH RISK CULTURE: THE UNICREDIT GROUP EXPERIENCE

24 Ralph Daals
AGILE AUDITING, REINVENTING内部 AUDIT AND CHANGING THE MIND-SET: THE RSA INSURANCE EXPERIENCE

26 Iván Martín Maseda
UNDERSTANDING MACHINE LEARNING: INTRODUCTION TO REGRESSION, CLASSIFICATION AND CLUSTERING

28 VISIT TO REINA SOFÍA MUSEUM

30 Naohiro Mouri
EMPHASIZE THE BASICS ELEVATE THE STANDARDS
Navigating Tough Waters: Maintaining Integrity

Annette Olofsson

Audit Challenges in Joint Operations: Exploring the Boundaries of Internal Audit. The Repsol Experience

Juan Carlos Martinez and Ian Hudson

Blockchain: Changing the Rules of the Game

Luis Enrique Corredera

Providing Reassurance Through Overall Audit Opinions

Manfred Kraff

How to Use Data Analytics to Massively Change Your Audit Approach: The Société Générale Experience

Louis Hedde

You Too Should Think Like a Hacker

Ymir Vigfusson

Integrated Thinking for Integrated Governance

Paola Schwizer

Applying Red Team Methodology in Cybersecurity Audits

Steve Rumble

The Allianz Audit Operating Model. Leading and Aligning Global Audit Function

Hervé Gloaguen

What Living in Space Taught Me About Life on Earth

Michael López-Alegría

The Atmosphere That We Have Expected

Manfred Kraff

Internal Audit of the Future

Martin Wiedemann and Rolf Spjelkavik

Discussion Panel: Challenges Faced by Internal Auditors in the Financial Sector

Henrik Stein, Juan Guitard and Sally Clark

Discussion Panel: Future Challenges for Audit Committees

Gilberte Lombard, Clare Thompson and Melvyn Neate
SANTIAGO BERNABÉU
Welcome to the Madrid European Conference for Super Internal Auditors. It is an honour for us that the ECIIA, the European Confederation of Institutes of Internal Auditing, should have entrusted the staging of the most important event of the year for the profession in Europe to the Institute of Internal Auditors of Spain.

I would first of all like to thank His Majesty King Felipe VI for agreeing to act as Honorary President, and for his consideration and courtesy towards the Institute. I would like to extend a cordial greeting in His name, and His wish for the Conference to be a resounding success.

We are also grateful for the support of the ECIIA. Of its President, Farid Aractingi, and of the Board. Support and commitment to the profession has also been demonstrated by our sponsors, without whom this event would not possible, and the 51 experts who will be sharing their experience and vision with us.

Lastly, I would like to express my thanks for the dedication and the huge efforts of the team at IIA Spain to make the Conference a success.

And, of course, I want to thank all of you, internal auditors from 52 countries, for attending this essential gathering of our profession.

Allow me to give thanks in particular to those of you who have come from beyond the borders of Europe: Koreans, Indonesians, Arabs, our brothers from Latin America and many other countries.

We have high expectations for this Conference, and trust that we will not let you down. Thank you to everyone, and welcome.

The internal auditors of Spain recall in particular at this time Eduardo Hevia, the Honorary President of our Institute, who passed away in July. He was one of the main driving forces behind our body and would undoubtedly have hugely enjoyed sharing these few days with professionals from so many different places, with one shared goal: the advancement of our profession so as to protect our organisations in the best way possible.

This year our goal is to “Pump up your Powers” as Super Internal Auditors.

Many of you will remember Ben Parker’s warning to his nephew Spiderman that “with great power there must also come great responsibility”.

Our responsibilities as internal auditors include keeping ourselves constantly up-to-date so as to protect the value of our organisations, and to ensure that they are responsible global players. Contexts of structural change as at present come with the emergence, evolution and interrelationship of risks and threats to organisations. Many of them are global threats and risks that affect what is also a global economy and society: changes in the geopolitical setting; regulatory demands; third-party risks; or risks resulting from digital transformation, etc.

To mitigate these threats, a sound risk management system is essential at any organisation.

MITIGATION OF RISKS

Contributing to the anticipation and mitigation of risks is one of our responsibilities: as experts in risk management and internal control we internal auditors are now, more than ever, trusted advisors and vital allies of the audit committee in fulfilling our task of providing the Board of Directors with assurance. This task is no less a task than the crossroads facing Europe today. The stability of Europe is threatened...
on various fronts, with increasing uncertainties for our organisations: internal political tensions, trade wars, migratory movements, management of natural resources, new economic models...
The level of mistrust that some citizens feel towards institutions and companies also needs to be reduced.

Today’s business model aims to re-establish an appropriate balance between the generation of trust, social legitimacy and the need to seek out new approaches, underpinning an efficient and humane economic and business model.

**GOOD CORPORATE GOVERNANCE**

Which is why it is crucial that we review corporate values and the establishment of good governance at companies. Good Governance fosters credibility, stability, and helps drive growth and wealth creation. It is an ethical and social matter and provides the best antidote against possible dysfunctions in the economic system.

Over the last 17-20 years, European corporate governance policy has generated initiatives that have helped establish basic common standards for Europe. However, they vary widely and lack a unifying framework.

This is where some of our professional value lies. There cannot be good corporate governance without effective Internal Auditing, since, despite regulatory disparities, as internal auditors we have the knowledge and tools to help directors to supervise appropriate control and management of business risks, in accordance with their guidelines.

Aside from the human and technical resources that we increasingly need to fulfil our mission, we also rely on our values, our superpowers: integrity; objectivity and independence to protect our professional judgment and impartial evaluation; confidentiality; and competence, doing our job in accordance with international standards for professional practice in internal auditing.

This very day the President of IIA Global, Naohiro Mouri, will in fact be inviting us to “Emphasize the Basics. Elevate the Standards”. STANDARDS and our ambition to improve are our key tools in combating the risks faced by our companies, the reference point allowing the Audit Committee to supervise our efforts. I mentioned just now the diversity and complexity of risks. And we cannot overlook the fact that on such a stage it is not enough simply to correctly diagnose the problems. Just like superheroes, we have to adapt and reinvent ourselves, fully understand the business, its aims and strategy, so as to keep it healthy.

We also need to bring in new values and skills. New powers to enhance our professional credibility, so as to offer advice and the best possible recommendations to the board of directors. Developing our powers means being better, being better prepared, advancing ourselves and our organisations.

In this Conference we have the opportunity to progress through sharing an analysis of the main risks that threaten our organisations and seen how to mitigate them. To advance by sharing experiences with other colleagues and learning from some of the world’s top companies, so as to improve the way we lead our teams; to maintain our commitment to the quality of our work, and to change direction and mentality, exploiting to the full the distinctive features of our leadership.

I would encourage you to learn, to share and to enjoy this unique opportunity for knowledge and professional networking. Welcome to Spain, welcome to Madrid. Make the most of your time here, and above all... Pump up your Powers!!

Our responsibilities as internal auditors include keeping ourselves constantly up-to-date so as to protect the value of our organisations, and to ensure that they are responsible global players.
His message was focused on the constant change in the modern world and the speed at which it is taking place, affecting all parts of the economy. These disruptions are here to stay, as he said, and have become a cyclical process in organisations. Over the last two decades there have been a number of crises that have had a really profound impact on our environment. We are trying to resolve each of these by establishing rules and regulations, which is making everything more complex, not only from the financial point of view, but also at the technical level in all the economic sectors.

How can internal audit act in this situation? By improving the performance of good governance through its professional activity. And to assume good governance the process of decision-making must be improved.

In turn, to improve this process a balance is needed between existing legislation and efficiency, thus achieving an executive management supported by what can be called an “unbreakable tripod”: Internal Audit, risk management and internal control.

These three functions must work together to achieve this balance between compliance and efficiency for the company.

The internal auditors 3.0, the latest generation of super auditors, must focus on a number of issues. One of them is independence, which is essential in our profession. To achieve it we have to be brave and “politically” incorrect, not only with respect to accounting records, but in all everyday activities involving our profession.

We must also be open, and have contact with all the organisation. Internal auditors are responsible for performance that is consistent with the long-term principles of the organisation.

Internal auditors must also have discipline, and be capable of facilitating the debates and handling antagonism well. They have the capacity to carry out an in-depth analysis and be relevant, but may also provide a holistic approach as internal auditors.

With independence we can achieve what Farid Aractingi defines as the “pragmatic value”; in other words, “making others listen so that we are really able to contribute the possibility of progress for the organisation. We must speak the truth with neither arrogance nor complacency, and be guardians of this temple.” Farid Aractingi said that “with the use of powers of attorney and improvements in the profession, internal auditors can take their place at the decision-making table, which is essential for helping the organisation to make real progress. That is what we are here for, to improve organisations and corporate governance.”

However, in what he defined as a journey, we have to accelerate and adopt the European dimension, which is achieved by combining forces to provide a new dimension in a global world where the countries of themselves are blurred, so adopting a broader and stronger European standpoint will help improve the profession.

The president of ECIIA ended his speech by giving as an example of this European collaboration the report Risk in Focus 2019. Hot Topics for Internal Auditors, drafted by six European internal audit institutes.

* Summary prepared by the Institute of Internal Auditors of Spain
TeamMate®
Analytics
Análisis de datos para cada auditoría

Disponible en integración en TeamMate Audit Management System y en uso independiente

Conozca más en TeamMateSolutions.com/Analytics o llame al +34659055806
When we saw the world’s economic and social development mid-way through the last century, we thought that it heralded the arrival of a new era; and it is true that there was a clear victory of the West during the Cold War. But now the world has de-Westernised, and is currently experiencing a decline and a shift of the global centre of gravity.

The centre of gravity is not on the Greenwich meridian, as Europeans always studied at school; rather, although it sounds a cliché, it lies in the Pacific: specifically, in the straits of Malacca, which is the natural connection between the Pacific and Indian oceans; very far from Europe.

Why there? It is a zone with a very high population; it has the highest rate of GDP growth in the world, and the majority of commercial transactions take place in this region. If we place Malacca at the centre of the world map, Europe is at the periphery of this current post-Western world, paradoxically, little more than 30 years after the victory of the West.

MEGATRENDS FOLLOWING THE DE-WESTERNISATION OF THE WORLD

Now we are faced with megatrends that allow us to understand the situation of the world better:  
1. The failure of the Anglo-Saxon world. The clearest example is Brexit, but it can also be seen in the policies of Donald Trump. The United States is abandoning multilateralism. There are a number of examples of this (the TTIP, the regeneration of the North America Free Trade Agreement, nuclear protection, the abandonment of the Paris agreements, etc.).
2. China is beginning to emerge and is becoming the most important global superpower of the 21st century. That statement requires qualification from the economic and commercial point of view, with the establishment of new multilateral institutions in parallel with existing ones. As well as its power on the ground, China is becoming a naval power with a presence around the world. It considers any conflict of vital importance to it, and it has an enormous presence in Latin America and Africa, and of course in Asia, which is its priority. For this reason it is expanding its presence in South China Sea against the U.S. And it claims it has rights over the zone of the Malacca straits by which it can assume complete control.
3. The strategic Bab-el-Mandeb straits that connect the Red Sea with the Indian Ocean. To their north lies Yemen, which is suffering from a civil war in which one of the sides is very closely connected with Iran. It would be a problem if these straits were to be under the control of Iran or its allies. To the south, in Djibouti, is the most important US military base in Africa, and a Chinese military base that is even more important. In the near future we will see the Chinese Navy everywhere, as is the case with the US Navy now.
4. The Middle East as a paradigm for the new non-Western world. History repeats itself, and some historic empires - such as the Russian one - are making a return; as are Iran, India, and Turkey. By way of example, in the Syrian civil war, the main countries represented are not the U.S. or Syria, but Russia, Turkey, Iran and, indirectly, Saudi Arabia. In other words, non-Western powers
THE ROLE OF EUROPE

What is Europe’s role in this situation? Its future is linked to the idea of the West, characterised by representative democracies, a free market economy, free trade in economic terms, and societies based on freedom and equality. Its role is even more important than before, and its strategic alliance with Australia, New Zealand, Korea, Japan, etc. will be very important for the future of the world and for our values. Europe began as an economic project, but has shifted to constituting a political project that has recovered the origins of European construction and is trying to recover the idea of confrontation between blocs by establishing a peace zone based on cooperation and solidarity.

Many people now think that Europe is not a good idea as a political construction, but it is important to recall that Europe has a history of success: we have constructed many elements of sovereignty in the EU, such as economic and monetary policy, defence of security, etc., to say nothing of the political content of the EU. Geographically the European Union is also a success. It began with six countries forming part and now there are 28 of us.

The failure of the project for a European Constitution was a turning point, followed by the need to digest three elements we still have to deal with: the expansion to the eastern countries; the ten years of recession in Greece, and the challenge of migration.

The problem is that we do not have real leaders. This affects the traditional model of making progress in European construction based on the Franco-German order. Everything in the history of European construction has been possible by the agreement between the French and Germans, despite the differences between them. France has a very pro-European government, but of itself it is not capable of pushing through improvements for European construction. And Germany has a very weak government in the run-up to the upcoming elections in Bavaria and the resulting new political agents.

Before, the Eurosceptics accounted for 10-15% of the MEPs in the European Parliament, but now they constitute a third. It is a new situation for Europe for which there is a lack of allies to push through European integration. Poland, Hungary, the Czech Republic, etc. are not very enthusiastic about contributing; and the Netherlands, Austria and Ireland, which were very pro-European before, are no longer so; and the same is true of the Nordic countries. In the south, Greece is not capable of introducing new ideas; and Italy, which is more European, has serious doubts, against the background of negotiations between the Italian government and the European institutions with relation to the public deficit and debt repayment.

So Spain and Portugal appear to be the only ones prepared to support the efforts of France and Germany to continue. The problem is not a lack of ideas on how to improve the governance of Europe; what is lacking is the political capacity to implement them. In this new world Europe could lose its relevance. If we are not integrated into a united Europe, each one of us on our own will lose relevance in the current world. To address the future of the West it is important to defend Europe as a political concept.

AN OPTIMISTIC OUTLOOK

Despite this outlook, there are grounds for optimism:

The world is growing at a rate of 4%, and this growth is synchronised between the different regions. In the last two or three years nearly all the regions have grown. The United States is growing above what was considered its potential, although there is a risk of overheating. China continues to grow at 6%, and India even more so. In a generation there will be more Indians than Chinese, and its growth will be 7%. Latin America is also growing, and in Europe we have begun to see significant growth, but in European terms (2-3%). There are exceptions to global growth [Venezuela, Turkey, Argentina, Brazil, Russia...] but in general the world is growing.

In part this is due to the ultra-expansionary monetary policy of a number of central banks, with interest rates that are practically negative and a great deal of liquidity in circulation, although in 2019 the interest rates are bound to rise. With respect to Europe, the confidence of the international markets will have to be based on the capacity of the EU countries to pay their public debt, which is the great problem. We have to grow to tackle the public debt and have a primary surplus in our budgets. Growth occurs with inflation, which is increasing, and we have to deal with the new economic scenario in these circumstances, and implement far more orthodox reforms.

Finally, there is another positive approach that has to be qualified: globalisation and digital transformation, or the fourth industrial revolution, which bring with them some extremely profound changes.

We have never had so many planetary connections as we have now. Never in the history of the world has there been such a large middle class. The world is improving; although many people continue to lose and we have to help them and integrate them into this global world. Good corporate and institutional governance plays a very important role in this as the path for addressing the problems of the world of today.

* Summary prepared by the Institute of Internal Auditors of Spain
The logic behind Risk-taking

The risks that can do you the most harm are those that are missing from the models. But how can we mitigate the risk of something we know nothing about? That is how Nassim N. Taleb, author of The Black Swan, takes us into the worlds of risk management from the perspective of someone who started playing with risk and taking it on in the role of a stock market trader to then focus on his theory as an associate professor of mathematical analysis and risk probability.

If it can help to apply a form of management in which you are penalised if you make a mistake. If you lose money as a stock market trader, you pay for it yourself from your own assets. When decisions have a direct effect on the person taking them and not on someone else. But you need experts for that. And what is a good expert? It is someone whose performance is assessed by a dose of reality: their clients and not their peers.

All this brings us to the core theory in The Black Swan. Nassim Nicholas Taleb invites us to visit two realities: “Mediocristan” and “Extremistan”. Knowing which “world” we find ourselves in affects how we should approach the analysis of risks in each one. The statistics studied at schools and universities is a theory for “Mediocristan” scenarios, but it means that the mistakes of banks and large companies usually occur in “Extremistan”. He gives the following example: if we randomly choose two people whose combined height is 420 centimetres, what is the most likely combination of heights from the two of them? The extremes will be highly unlikely - having one very, very tall and one very, very short - right? This takes us into the world of “Mediocristan”. Height follows the catastrophe principal - major deviations are not caused by a single event but rather by several events.

On the other hand, what is the most likely combination if we choose two people with a combined total of 36 million dollars? 18 + 18? In this case, it would be 36 million minus 1 dollar and 1 dollar. Welcome to “Extremistan”.

In other words, if a bank/company has a big problem involving billion-dollar losses, where will the problem come from? From thousands of one-dollar mistakes or a single billion-dollar mistake? The latter is more likely. This is why most losses are caused by very few events. The banking crisis of 1982 was repeated in 2008. When will the next one be? This is what Nassim Taleb refers to as the mistake of naive people.

Operation Risk

The operation risk in different sectors is Extremist and stems from a very short series of events. However, we are used to analysing events from the “average” and Nassim Taleb warns us that, if you invest in a market, you are not going to receive the market average. What would you say is the average profit of 100 people betting 1,000 dollars over eight hours? To calculate this, you would need to go to the casino 100 days in a row. However, if you go bust on day 27, you don’t have a day 28. And if there is even a small likelihood that you will go bust, you are sure to go bust.

This is why we need to understand real life in order to understand the logic behind risk. Risk should
be approached from a dynamic (over time) perspective and never a static one, and we are taught static techniques at university. Furthermore, if the risk is not static then the historical distribution is not empirical and this leads us to the “Lucretius Problem”: the tallest mountain is the tallest mountain that anyone has seen. The Egyptians used to make marks on the river to show the highest level the Nile had ever reached. The bank stress tests used to be performed according to the last huge collapse experienced by the stock markets (10%) until, in October 1987, they fell by 24% and that became the new rule. But we now know that the highest and lowest water marks are going to be beaten (extreme value theory) meaning that, to avoid “the Lucretius Problem”, the worst case scenario to have materialised should never be used as a basis but rather the worst case scenario that could happen in the future.

**DYNAMIC RISK ANALYSIS**

It should also be considered for this dynamic risk analysis that we must understand the psychology of people and “scaling” theory - where a small village is not the same as a large city and a single person will not behave in the same way as a group of people - and even that the average here will not be determined by group behaviour but rather often by the minority in cases where production costs are similar or low (for example, if gluten-free food is cheaper and similar in taste, most food will probably end up becoming gluten-free). Hence, people tend to think that markets are moved by consensus between participants when, in actual fact, they are moved by a highly motivated minority.

In conclusion, Nassim Taleb encourages us to start moving towards the “Mediocristan” and “Extremistan” theory, and thereby focus ourselves on survival given that mankind has survived 300 million years thanks to survival paranoia, and that tells us “there is nothing irrational about paranoia, in fact we should be more paranoid”.

Nassim Taleb encourages us to start moving towards the “Mediocristan” and “Extremistan” theory, and thereby focus ourselves on survival given that mankind has survived 300 million years thanks to survival paranoia, and that tells us “there is nothing irrational about paranoia, in fact we should be more paranoid”.

And so we ask ourselves, “how can we tackle uncertainty then?” Nassim Taleb says that, if you don’t know the situation, you see things little by little; if you don’t know what’s happening, take care with your business, you see things little by little. That is how you avoid “Extremistan”. There is only one way to tackle uncertainty and that is with the way YOU behave, even if you never come to understand the situation that surrounds you.

*Summary prepared by Ana Minguet Blázquez*
The two decades to 1970, characterized by the adoption of the Bretton Woods-negotiated monetary order, witnessed a significant reduction in domestic economic crises as well as banking crises. The period also straddled the controversial launching of the Nobel Prize in Economics in 1969, which drew (and still draws) worldwide attention and the adoption of prize-winning innovations in economic theory. The contemporaneous accession of increasingly rigorous mathematics into the science of economics led to the establishment of financial mathematics as a separate branch of learning, as well as the quantification / measurement of risk. The arithmetic of the introduction of mathematics into economics required the use of past data to evidence the explanatory power of newfound empirical relationships. Besides the explicit assumptions adopted in these accomplishments, there was the implicitly infused premise that past data constitutes a good fit for modelling future outcomes. The unravelling of the Bretton Woods order post 1970 beheld the re-emergence of domestic economic crises, as well as banking crises. Technological and communication innovations, together with an unprecedented number of countries embracing deregulation, democracy and open / semi-open domestic economies, combined to produce the most interconnected global economy in history. Still, not only did / do the characteristics of the post Bretton Woods global economy - floating exchange rates, application and scale of derivative instruments, number of open economies, ease and speed of capital flows, velocity of communication, re-introduction of China into the global economy and others - differ markedly from those that prevailed during Bretton Woods, the most powerful economies’ fiscal positions and outlooks also contrast incalculably from the conditions that existed in the two decades to 1970. Examples include:

● the current debt levels of these countries, which are at all-time highs during times of peace;
● their commitments to social security (unfunded) and health care (unfunded) - in addition to the longevity risk they face;
● inequality levels, which are at the opposite end of the spectrum compared to the positions at the commencement of Bretton Woods;
● inequality’s intersection with populism, the ability to vote and democracy;

In an ever increasing technological environment, in which any analysis requires access to an enormous volume of data from different sources, what responses can forensic technology provide for the challenges faced by the internal auditor?
With regard to endogenous risks, fraud, the corporate great white shark, is one of a company’s main risks due to the combined impact it can have on both economic losses and reputational damage. Simply speaking, a relevant fraud case, irrespective of the amount of economic losses, can put a robust company out of business as illustrated by multiple cases.

Considering that risk can be avoided and mitigated by using a window of opportunity as, in 65% of cases, fraud is committed by employees who have been with the company for more than six years, according to KPMG’s Global Profiles of the Fraudster report.

In order to enhance and implement a real anti-fraud strategy a number of potential misconceptions with regard to fraud should be avoided:

1) The rules of the cost-benefit ratio

KPMG spent 12 years performing extensive academic research to find an empirically proven, scientifically defendable methodology to overcome the paucity of data challenge in modelling future risks. The resultant methodology, which applies the sciences of expert elicitation, behavioral economics, graph theory and mathematics - known as Dynamic Risk Assessment - performed superior to other modelling techniques in identifying the combination of a modest (3% to 5%) market correction plus a rating downgrade plus an increase in borrowing costs as a retail bank’s most severe and imminent (aggregated) risk ... significantly ahead of the onset of the Credit Crunch with the collapse of Lehman Brothers on 15 September 2008. This methodology identifies future risks, including unprecedented risks, which result from combinations of individual risks (i.e. recognizing their interconnectedness and causal relationships to other risks), future potential tail events, the opportunities to be found in systemic risk networks and the combination of discrete risks that present the greatest systemic threat to organizations. It also distinguishes between individually benign risks that can trigger severe aggregate outcomes, and those individually benign risks that are unlikely to trigger severe aggregate combinations of risks.

**FRAUD RISK**

An event that can take you out of business is unusual, rare and unlikely; if it appears suddenly the effects can be devastating. As such, in today’s world of constant change, we must be prepared for the probable and the possible, as well as for the improbable and the impossible.

With regard to endogenous risks, fraud, the corporate great white shark, is one of a company’s main risks due to the combined impact it can have on both economic losses and reputational damage. Simply speaking, a relevant fraud case, irrespective of the amount of economic losses, can put a robust company out of business as illustrated by multiple cases.

Therefore, a real strategy aimed at preventing, detecting and responding to fraud is required,
Data analysis will grow more effective with the improvement in the quality of the data processed and the application of artificial intelligence systems, which enable an analysis of unstructured data such as text, images and videos, which until recently were impossible to analyse.

The varying severity of risks can be identified both individually, where they can be more or less aggressive, and collectively, where something individually harmless can become a time bomb in association with other risks with which it often goes hand in hand or can remain something simple to manage.

Fraud is a good example. From an economic point of view, it can have a minor impact, but if the case appears in the news and reputation is affected, then the impact on stakeholders’ perception of how a company does business can be substantial.

THE ROLE OF TECHNOLOGY

In addition, the role of technology is critical to preventing the risk of fraud. However, technology is used much more to commit fraud than to detect or prevent it; herein lie opportunities for future improvement.

Particularly noteworthy is the growing importance of new technologies, especially data analytics, in the prevention, detection and investigation of irregularities and fraud.

The statistics are illustrative: advanced data analytics reduce fraud detection time by 58% and measured losses by 52%, according to the latest Report to the Nations. Examples of the application of data analytics to fraud prevention, detection and investigation are increasingly numerous and varied. One way to see the significant value of data analytics in fraud prevention is by analysing impossible transactions, which are transactions that should not occur (for example, those that exceed a certain monetary limit in the absence of approvals) but do occur nevertheless.

Data analysis will grow more effective with the improvement in the quality of the data processed and the application of artificial intelligence systems, which enable an analysis of unstructured data such as text, images and videos, which until recently were impossible to analyse.

At present, companies only analyse 1% of all unstructured data they own, suggesting that we are failing to take advantage of the possibilities of data analytics to prevent fraud. However, we all agree that advanced data analytics will be critical in 21st century risk management to identify fraud cases before they lead to destruction. It allows us to reach places where the human mind cannot go, all this without forgetting the human factor.

The reality is that technology helps but does not replace people – to put it in other words, technology is necessary but not enough.

This is the biggest challenge we are now facing, as it is necessary to seek out the best combination between technology and human resources, in order to distinguish between a distance dangerous fraud event and the implementation of an efficient fraud risk management strategy.
¿Quieres saber cómo acceder?
Escríbenos: servicioscliente@iai.es
o llámanos: 91 593 23 45
All internal audit departments feel the same pressure from stakeholders to be more efficient executing their projects while at the same time they still must cover a different and constantly changing risk universe. Software and consulting vendors are also promising a new golden age if we embrace the new technology with which they provide us. At the same time these pressures take place, the auditees face a similar challenge to adapt themselves to a digitalized and automatized new paradigm. This leaves us under a perfect storm scenario. We are not sure about the storm direction, neither its duration, but there is one thing we know for certain: the traditional audit role and the traditional auditor have a short useful life span.

To manage this scenario, we are working hard in Ferrovial to identify the storm characteristics, analyze our boat to ascertain our strengths, benchmark what other vessels may be doing, and ask the experts for advice. This process has led us to define different actions plans. We soon realized that some plans were not feasible, while we had to put others on hold as we think they are feasible but there is an element that is not yet mature enough to help us deliver value for money today. Fortunately, we do have some good news that may be producing real, tangible results in the medium term.

**DIGITALIZATION TRENDS**

Adapting to increasingly digital market environments and taking advantage of digital technologies to improve operations are important goals for nearly every business. Yet, few companies appear to be making the fundamental changes their leaders believe are necessary to achieve these goals, among others: developing cross-functional teams, having long term planning horizons, locking digital skills, developing leaders with digital ambition, and finally, allocating sufficient budgets. To date, the most popular digitalization initiatives are related to: The Internet of things, Collaboration platforms, Cloud, Big data, Robotics and Virtual reality. However, we believe technology is useless if employees are not considered. When facing digital transformation, companies should not undervalue the importance of cultural change. Digitalization is doomed to failure if employees are not embarked on the process and the best digital talent is not brought in. In addition, companies should also adapt themselves to the new digital worker profile, that usually shares the following characteristics: prepared for solving IT incidents, works remotely, uses light devices, shares information through collaboration platforms and works in the cloud.

**THE ROLE OF INTERNAL AUDIT**

Internal Audit needs to continue delivering value as organizations evolve. Digitalization should not only be automating internal audit processes, but also about delivering new audits as businesses evolve towards digitalization of their practices and processes. The main areas of growth that we have identified are focused on: Information
governance and Data Privacy, cybersecurity, mobile technology, vendors, fraud detection through data analytics and continuous audit (more feasible for standardized processes than for others where auditors’ judgment is still required). The desired panacea is up-front prediction and identification of behaviors to focus on specific areas of concern, plus improving internal audit management tasks (automation of audit universe, reporting, etc.). Even in the worst-case scenario, automating recurring tests will save us time, help us focus on more value-added activities, reduce error rates and provide enhanced result assurance to our stakeholders.

ROADMAP IN FERROVIAL

Our roadmap in Ferrovial follows the following steps:

Brainstorming exercise to identify areas subject to automation. Lesson learned: IT tests are usually left aside as their recurrence and repetitive nature is lower. Still, there is room for automation in many tests (i.e. user and access management areas). We will need to tackle IT test automation in a future wave as we have now focused on financial and fraud tests and on audit management matters. Assess priority considering potential time reduction and benefits from lowering error rates. In addition to time-consuming tasks, there are areas far more exposed to human error that will take advantage of automation. Those are the areas to which we have assigned higher priority.

Identify affected supporting systems. Lesson learned: Digitalization is highly complex in decentralized IT environments with multiple systems and data structures. Also, digitalization is highly data integrity-dependent, the more inaccuracies in data sources and relationships, the more useless it gets.

Assess whether there are any similar automated tests performed by other business or controlling functions. Lesson learned: In mature organizations, business and controlling functions usually perform automated tests to ensure processes accuracy, especially on those susceptible to fraud. Is it the business that should feed internal audit or the other way round? Either way, communication business-internal audit should be permanent, so that tools and checked results can be shared.

Analyze the best supporting technology/tool for each item. Internal VS external support must be firstly analyzed. Sometimes, Excel macros or scripts can be internally developed to support the planned tests (proper time and resources allocation is needed). Assessment on the feasibility of external options has led us to different actions plans, we already know that some of these are not possible, while others are being put on hold as we may still think they are feasible but there is something that is not mature enough yet. We have continuously changed deadlines and budgets.

Along this journey we have also noted that the organization counts on similar technology that we are using so we have taken advantage of it to negotiate better contractual conditions with the vendors. Some examples of the tests that we have automated are:

- Audit universe and risk matrix (Robotics).
- Extraction of all Cost Centers’ Financial Statements and Budget (Conecta).
- Audit report interaction (Office + SharePoint).
- Follow-up of quality questionnaires (Excel Macro).
- Duplicated invoices (Conecta).
- Abnormal purchases and 3-way-matching (Business BI).
- Abnormal Overtime (Data Lab).
- Invoice ageing (Excel Macro).
- Debt recalculation (Excel Macro).
- Continuous auditing and sending to business for review (Conecta).
- Personnel expenses (SAP HR automated report).

Companies should also adapt themselves to the new digital worker profile, that usually shares the following characteristics: prepared for solving IT incidents, works remotely, uses light devices, shares information through collaboration platforms and works in the cloud.

- Users and password analysis (Scripts).
- IT Services KPI & SLAs fulfillment (Excel macro).

CONCLUSIONS

The traditional audit role and the auditor have a very short useful life span. However, are all auditors ready to embrace the right skills to effectively evaluate digitalization risks and controls? Digitalization of internal audit internal process has just started. There is still a long way ahead. Along this path we need to manage the traditional auditor’s resistance to change, the potential misunderstanding of digitalization from the audit leadership and the lack of the auditor’s right skills to effectively deal with digitalization.

Nowadays, value for money is difficult to find, as high customization is needed to get the optimal results. Final reflection, do we really want to make everything automatically predictable and auditable? Is it that possible? We want to leave you with a final optimistic message, we are absolutely convinced that auditors’ judgment will always be needed.
Risk culture attains the behaviors, the underlying values and the beliefs of each component of the organization and steering, influencing and measuring behaviors represents a significant challenge of the Board.

Promoting a sound risk culture in alignment with the espoused values leads to several remarkable benefits. A robust risk culture contributes to the viability and sustainability of the company and to fulfil long-standing expectations of stakeholders.

The concept of risk culture is unavoidable related to a concept of long-term sustainable goals whereas significant flaws of risk culture have often proved a direct link with the achievement of compelling short-term economic/commercial results.

Owing to such considerations, each Board is called on to have a deep understanding about the risk culture spread in the organization and about the gap versus culture objectives falling in the perimeter of strategic objectives.

A clear picture of consistency between the set-out and planning of economic/business targets with a sound risk taking and risk culture should represent a cornerstone of Board Members consideration.

**CORPORATE GOVERNANCE**

In several situations of risk culture flaws, sanctions have often affected senior and middle management with minor impacts on the Management Board members. However the roots of risk culture are deeply connected with a robust corporate governance (under the direct accountability of the Board), called to ensure a strong bond between a sound risk taking and corporate values promoted by the organization.

Drivers of a sound corporate governance, risk culture and effective management of conduct risk, such as: tone from the top; accountability; open communication and challenge and incentives, need to be implemented through a proper risk culture framework, capable of linking organizational business dynamics with espoused values.

Several sound indicators of risk culture have already been identified by regulatory provisions and best practices over the years. Incentives policies (to link to long-term sustainable economic results); effective consequences management (to adopt timely and effectively and envisaging both positive and negative outcomes); sound vetting procedures and clear career paths; open and extensive wide communication flows represent just a few instruments which might and should be distinctive of a sound risk culture. Playmaker of a sound risk culture is the Board in its role of strategic body of the company. SREP guidelines pinpoint the close bond between business model and corporate governance clearly underlining the significant link between a sound risk culture and a viable and sustainable business model.

Doubtless, contributing to provide assurance on risk culture represents a high added value for the organizations. Internal Audit might serve this purpose effectively moving towards an assessment which analyzes, among others, the consistency between day to day behaviors, aimed at achieving performances and

**SERENELLA DE CANDIA**

CHIEF AUDIT EXECUTIVE AT UNICREDIT GROUP
economic targets, with espoused values. Clearly the assessment on such matters implies that, besides more “traditional” topics of assessment (assessments on incentives and remuneration schemes; consistency between RAF and granular business targets; etc.) a specific focus is also turned on the processes related to the set out and implementation of strategic plan and commercial processes.

**PROVIDING ASSURANCE**

Providing assurance on risk culture means therefore not only gaining a positive assessment of typical drivers of risk culture developed by risk management compliance and HR functions, but also to get a deep understanding on how business targets are achieved. This should imply a substantial knowledge in terms of plausibility of budget and strategic planning figures with sound commercial practices.

Providing assurance on a sound risk culture for the Internal Audit envisages a clear view on how risk management, compliance and business lines address their role respectively in the monitoring of risk culture framework, in the management of conduct risk and in the self-awareness and management of risks.

Providing assurance on a risk culture means to report effectively on risk culture flaws and weaknesses to the Board pinpointing timely breaches in espoused values and ethical behaviors, even when certain behavioral attitudes benefit from the achievement of key business results.

Getting ready to report effectively on risk culture also means to build-up in sociological skills and techniques and to properly review the coverage of risk culture topics through a thorough analysis of audit universe. Audit techniques at the same time should be enlarged to include surveys reflecting risk culture matters and work programs are expected to incorporate control objectives and indicators linked specifically to risk culture.

Breaches in risk culture impact not only on reputational risk but also reflect on the bottom line through the consequences of fines, sanctions and legal causes proceedings. Therefore a sound risk culture should be considered more than ever as a company asset which needs to be safeguarded and which cannot be easily “restored” or “replaced”. Working in sectors with lower margin trends or highly competitive environments means to trigger potential bad behavior due to high commercial pressures.

**OPEN DISCUSSION**

Board members, risk management, compliance and internal audit should consider carefully such implications respectively in the setting of strategic goals and risk taking (Board) and risk assessment and approach (risk management, compliance and internal audit).

From this perspective, it would also be worthwhile getting the chance to have an open discussion with regulators and rating agencies on what is the value/price of a sound risk culture. Possibly with a “sounder” interpretation of such topics, risk culture might really become an increasingly recurring point of agenda of the Board as it deserves.

Playmaker of a sound risk culture is the Board in its role of strategic body of the company. SREP guidelines pinpoint the close bond between business model and corporate governance clearly underlining the significant link between a sound risk culture and a viable and sustainable business model.
In a world where change and disruption are becoming the norm, RSA Internal Audit realized they needed to disrupt themselves to remain relevant and impactful. They did not take a traditional approach to transformation – there were no project plans, champions or documents detailing the changes it would make.

They didn’t have deep pockets for consultants given the agenda of strategic rationalization, cost reduction, and operational turnaround across RSA – constraint was a key driver of innovation. Not afraid to challenge the status quo or do things differently, they searched well beyond traditional audit practices and took ideas and inspiration from cutting-edge companies regardless of industry and function, including Google, Pixar, Spotify, and Jim Collins’ book ‘Good to Great’. From this, a forward thinking function is emerging that has embraced ‘agile’ and encourages innovation.

Ralph Daals, Group Chief Auditor of RSA Insurance, talks passionately about the journey he and his team have been on for a little over two years now. Reflecting on their journey he says there were four main interconnected ‘building blocks’.

“The first was about simplifying and standardizing what we do and when we do it. We were looking to minimize complexity and distractions to allow us to spend all our time and efforts on what matters most. Critical in this process is to be comfortable to stop doing things.”

“The second was about increasing relevance and timeliness of insights and interventions. We shifted our traditional annual planning process towards a flexible 6+6 planning process to run more in parallel with changes in the business and emerging risks.” At the same time the team brought plan delivery in line with reporting to Executives and Non-Executives, cutting the time from ‘findings to committee reporting’ to a real minimum. Daals notes “Our team now delivers 100 percent of our plan every quarter, which was unheard of in the past.”

“The third was about implementing an ‘AsOne’ operating model, inspired by Deloitte”, Daals explains. “We broke down the silos that typically exist in an international function and eliminated traditional reporting structures and hierarchies.” RSA internal audit consists of 60+ professionals based in key cities across three regions: UK, Ireland and Middle East; Canada; and Scandinavia. “Our model facilitates a high level of connectivity and collaboration across regions and means we work together as if we are all sitting in the same room.” Consequently the quality and consistency of output and coverage; sharing of best practices, and efficiency improved.

“The fourth was all about building a high performance culture”, Daals says. “Which for us is about creating an environment where we can attract and retain the best”. RSA was inspired by Google’s approach to talent, who made hiring remarkable people their single most important activity, and worked closely with a leading performance company [PlanetK2], who supported British Olympic teams to improve both collective and individual performance.”
AGILE FUNCTION

“All these steps came together to create what we now characterize as an agile function” says Daals. “In simple terms agile for us is about being dynamic and flexible. It is about our ability to anticipate, respond and continuously improve. Both to meet our stakeholders’ needs and the evolving world,” says Ralph Daals. “Agility should be embedded in the mind-set, culture and values of the team; processes and methodologies then follow naturally. It’s about having a team that can continuously improve. That does not mean that everything is perfect, but it’s about how we adapt and respond to these challenges to get better.”

Inspired by Spotify’s agile culture, RSA turned their structures on its head, to center on “squads” – self-sufficient groups of up to six people selected for their suitability for the audit or task, regardless of location or level. A squad is responsible for an audit or project and has significant autonomy over how they organize themselves and how to best deliver an outcome. Leaders support squads as needed to deliver their outcome. The following gives a view of how it comes together (see picture).

To encourage collaboration and open communication, RSA introduced “ceremonies” – daily stand-ups, weekly catch-ups, fortnightly showcases and retros & sprints.

CLEAR ACCOUNTABILITY

“As we move along on our journey, our accountability always remains front of mind”, Daals reflects. “Every six months we ‘look back’ across our business through the lenses of issues raised by others, risk incidents, and material external events. We challenge ourselves honestly – ‘where were we?’, ‘did we pick it up?’, and if so, ‘did we report it appropriately?’” Learnings identified are widely discussed and fed into the continuous improvement of the function.

This focus on accountability and improvement is further reflected in the quality assurance reviews performed by Deloitte and “BrainTrust”, a forum that collects constructive feedback from all levels in the team.

AUDITORS OF THE FUTURE

With the company rapidly changing with innovations around big data, digital, robotics and more agile developments came a new profile of risks. This meant RSA needed to attract a new type of internal auditor with skills important to the organization of the future; as a result the team brought in a web & app developer and criminologist.

Daals continues, “It is however important we not only bring in new skills, but make sure all our people are set up for the future. So we upskilling our people in ‘new world risks’, including the basics of coding; auditing agile developments; and playing through mock crises such as a cyber-attack”. In terms of progression, Daals points out “Typically, people can’t progress until the person above them leaves. But you really don’t want great people having to leave in order to grow, so we have no fixed number of people per level. In our model, if someone is ready to be promoted, they are. There’s no need to wait for a vacancy.”

WHAT’S NEXT?

“It has been a good journey so far”, Daals says, “Our feedback scores have consistently gone up; our people are in high demand by the business; and we have a much more agile and forward looking model. But it is fair to say it doesn’t stop here. We have identified, for example, seven ways of injecting innovation into auditing, including stress-testing the control environment and risk event and scenario based auditing. As long as it supports our purpose and we keep an eye on what we call ‘audit risk’, we won’t hesitate to give it a go!”

Further, RSA – inspired by Pixar – is applying an iterative, ripple-based approach to innovation which encourages people to take small, regular steps to improve and accept failures. “We are working towards a culture where people aren’t afraid to fail, Daals says. “We’re not entirely there yet, but people aren’t punished for trying new things. If you do fail, fail fast, learn fast, and never compromise on outcome.”
Machine Learning, as it is referred to, is not as recent as its name appears, but instead, it goes back to the 50’s, when the computers tried - and succeeded - to trick the user into believing that it was not a machine but a person, under equal conditions. This is known as the “Turing Test”, and was also the first step for, a few years later in 1958, the creation of the first artificial neural network by Frank Rosenblatt. Thereupon, Machine Learning was defined with the basic but accurate quote: “as the field of study that gives computers the ability to learn without being explicitly programmed.”

Following the line of history, it’s not until the arrival of the millennium when the importance of Machine Learning at a commercial level is taken into account, that is, since then it begins to be exploited and adapted to the demands and needs of companies. Machine Learning has opened a door to a new world of possibilities that could not be contemplated before, especially in relation to industries where the availability of data is only increasing. This is the case of Google, a company that gave Machine Learning a very particular use in 2012, using the GoogleBrain lab to analyze all the YouTube videos to detect those containing images and clips of kittens.

Beyond the search for adorable kittens, understanding the basic principles of the new techniques of Machine Learning has become a necessity in the decision making of a company today. It is an unprecedented competitive advantage. It is about transforming years of experience in an industry based on predictive models, supporting all the decisions to be made. It is about evolution. It is about Machine Learning. Let’s start.

The three most common techniques are Regression, Classification and Clustering, which are in other words, the techniques necessary to be able to engage a conversation about Machine Learning with data professionals.

**REGRESSION**

Regression is in simple terms, a prediction technique. According to the data and the variables that are offered, the unknowns are cleared - or rather, estimated. For example, to know the price of a specific house in a specific city, you can use the Regression technique. Obtaining the independent variables, in this case, the data of the year in which it was built, the square meters, or the number of bedrooms, among others; with an associated dependent
variable, following the example, the price; you can find out how much the house would cost. Furthermore, by performing this analysis, the value of the independent variables is ascertained, that is to say, how the price of a house varies depending on its size or its quality. While we can say that the Regression technique answers the question “how much?” it can be declared then that Classification responds to yes-or-no questions. This means that the margin of error can become more complex to estimate. In other words, Regression can create results that are not exact, but are approximate enough to be valid or useful. But that is not the case with the Classification technique: it’s either white or it’s black, there’s no gray response available. A day-to-day example would be the decision the email software takes to send an email either to the inbox or to the spam folder.

**CLUSTERING TECHNIQUE**

Finally, there is the Clustering technique, which is part of the group known as Unsupervised Learning, used for statistical data analysis in many different sectors. This last technique differs from the previous ones, leaving behind patterns and numerical predictions, it goes further creating new data. It begins its operation by dividing within categories those data that have similar characteristics, which are called clusters, as could be expected. An example to expose the use of this technique would be a store, a small business that wants to continue expanding its business. For this, the owner decides to analyze the characteristics of the clients and devise a commercial strategy based on the data obtained. However, it is not possible to create a strategy for each client. So the customers are divided into different groups such as: those who bargain, the undecided ones and the wasteful ones. Based on the characteristics of each person, you are introduced into one of the three clusters created, and the commercial strategy that best suits your personality is applied. These are the three techniques that form the base of the Machine Learning pyramid. Iván Martín Maseda was the speaker who gave the lecture about them last Thursday, October 4 during the Super Internal Auditors 2018 event that took place in Madrid. As Chief Technology Officer at the Spanish Startup Binfluencer, in addition to being the Academic Director of the Data Science Bootcamps at IE Business School, he was the most suitable to speak on the subject, since he works and teaches Machine Learning daily. In addition, his motivation and passion make him the perfect speaker.
VISIT TO REINA SOFÍA
MUSEUM
This profession has changed my life, and now I can help others to see what I do. Twenty-five years after beginning as an internal auditor I still have the same level of commitment. And I still insist on raising the level of rules and standards. That is what I want to do during my presidency of the Global IIA: highlight the most basic aspects and raise standards, because it is of critical importance to respect them. Companies are facing many risks and difficulties, and I want us to return to the fundamentals, because only in this way can we continue to be relevant in the future.

We need standards to construct the foundations on which we can defend our professionalism. The Standards are like the plan that allows internal auditors to improve governance, risk control and processes. In the founding era of IIA, the statement of responsibility was a milestone in the history of our profession, but only the start. Soon it became part of the International Professional Practices Framework (IPPF) for internal audit. The basic principles are also very important. Internal audit evolves constantly, as reflected by the IPPF framework, and with it we can begin to construct that office block I was talking about at the start. We have to achieve assurance, advice and important ideas that serve us as critical engineering.

**THE ACTIVITY OF INTERNAL AUDIT**

What can we say about the activity of internal audit? That it must be independent, and that the internal auditors must have the necessary skills to carry out their activity. Internal audit must assess efficacy and contribute to the improvement of risk management processes. Our standards serve as a framework for constructing our office block, for constructing a successful profession. The standards are also in the 10 Fundamental Principles of accounting, and internal audit can comply with them to make progress. While the project manager of our office block ensures that the standards are correctly executed, you have to comply with the principles. It is not difficult if you are convinced about what you are doing, and allows you to identify how to document the evidence, because if not the building collapses. Our certificates demonstrate that we are committed to our task. The CIA and other certificates are the details of the real architects which allow them to reach higher and contribute value to the organisation. If we consider ourselves to be a profession we have to think about what constitutes a profession. Doctors, lawyers, accountants... they differentiate or are selected because...
people trust in their experience and because they comply with a series of standards and have a certain quality as professionals. The same is true for internal auditors. Complying with the Standards means moving along the correct path. This profession is fascinating and very varied. It is a continuous learning experience. Twenty years after arriving here I still have the same enthusiasm and same commitment. The Standards have helped me during my career, and in the future they will be even more important in face of the new challenges and tools for our work.

Quality Assurance

In addition, there is an element of the Standards which is perhaps more difficult to comply with: quality assurance. Accept it like a medical check-up, and let’s comply with the supervision of our quality to achieve conformity. There may be things that we are not doing well. Assessing the quality of our department, of our work, is key to becoming better. In addition, the Audit Committee has to understand what the criteria are for assessing us, measuring what we do; and their fundamental tool is the Standards. They have to know the Standards, and we must be able to influence them so that they see it in the same way.

But we should not forget that the core of what we are doing is not to achieve conformity with the Standards. They are simply the means for improving the core of our activity: giving value to the business. Only then will we be relevant.

* Summary prepared by the Spanish Institute of Internal Auditors through an interview with the subject
With the EU GDPR coming into effect on May 25, 2018, internal audit departments are also affected. While this regulation and its principles do not restrict the audit rights per se, they do give compulsory guidance as to how audits are to be performed. Similarly, audit departments will be tasked with examining company compliance with privacy principles and provide corresponding recommendations.

PERSONAL DATA

The EU GDPR applies whenever personal data is processed. While in the past, audit departments might have argued that they were not processing personal data, it is most likely that such a statement does not hold up under the new regulation. On the one side, the concept of personal data is broad. Article 4 (1) defines personal data as any information relating to an identified or even identifiable natural personal. This means that indirect information that leads to an individual is also of relevance, such as a user ID. On the other side, the concept of processing of personal data is equally extensive (ref. article 4 (2)) and involves, amongst many other things, the collection, storage and usage of such personal data (i.e., activities that auditors typically perform when doing their fieldwork). Article 5 defines the basic principles for personal data processing, such as its lawfulness, fairness and transparency and whether data processing is limited to what is necessary in relation to the processing purpose. The principle of accountability stipulates that processing is compliant, intentional, well-structured and traceable. In the end, the EU GDPR requires internal audit departments as corresponding process owners to define rules for processing personal data while abiding by the basic principles, therefore enforcing the concepts of privacy by design and by default.

IIA STANDARDS

Adherence to IIA standards already gives a sound basis for EU GDPR compliance. Still, it is advisable to challenge the departmental processes according to the principles and concepts mentioned above to identify where changes or adaptations to the audit handbook are needed. Corresponding communication and training of the
Auditors would also be a logical next step and should not be restricted to only when the EU GDPR is new. Ongoing awareness campaigns will also help foster a sound level of data privacy attitude for the future. The following list gives you a number of examples of topics that should be included in your analysis and may serve as good guidance for your review of audit approach and processes:

- Assess data privacy risks to persons vs. legitimate interests of the company.
- Verify the adequacy, necessity, appropriateness, and minimization of personal data usage during audits.
- Mention access to personal data in the audit assignment whenever personal data plays an important part of the audit scope and/or audit activities.
- Only collect personal data as defined in the scope of the audit.
- When selecting samples, define in advance what your selection criteria are.
- Analyze the data according to the topic/question you want to answer, but not user specific. Specific users should only be of interest for the clarification of first audit results.
- Request data already in an anonymized or pseudonymized format. If not possible, separate the task of collection/anonymization from the task of data analysis within the audit team.
- Restrict access to the data to an absolute minimum and have separate folders for sensitive audits.
- Remove all collected personal data not relevant for the audit (personal e-mails, hard disk duplicates).
- Do not store audit data in the easily accessible directories.
- Do not mention individuals in audit reports, use department codes.
- Define audit report distribution lists and keep them to a minimum.
- Define rules for the deletion of audit data.
- Implement technical and organizational measures in your audit software, ensuring an appropriate level of security.
- Make sure you can demonstrate adherence to GDPR standards not only through coverage in the audit handbook, but also for the single audits when drafting the audit assignment, doing the audit fieldwork, and publishing the report. Equally as important is to define regular checks on EU GDPR compliance as part of your quality management processes.

**Areas to Include**

When assessing a company’s compliance with EU GDPR requirements, the same principles and concepts previously discussed also apply. It is advisable, however, to assess the topic on a larger scale and include the examination of the following areas:

- Data Protection Strategy and its approval, implementation, and communication,
- Rules and Regulations, including the implementation of internal and external requirements and a check on adherence and controls,
- Organizational questions, including the structural and process organizations, data protection assessments and escalation paths in case of infringements,
- Communication and Processes, including awareness campaigns, trainings of employees and the definition/monitoring of processes and;
- Reporting (i.e. regular and event driven reporting lines).

In the end, the EU GDPR requires internal audit departments as corresponding process owners to define rules for processing personal data while abiding by the basic principles, therefore enforcing the concepts of privacy by design and by default.
Through his own personal experience he exemplifies an aspect deemed vital in this activity, namely an understanding that anyone can innovate, even himself, having begun his professional career as a lawyer. It is not a specific function of engineers or tech workers, but must be instilled in the culture and mentality of companies. Although they are inevitably associated, innovation is not the same as technology, but instead means bringing in some new element, which can cover many different concepts. Clearly, technology serves to accelerate these transformations.

**OPEN INNOVATION**

In the specific case of Telefónica, they divide their strategy into two separate branches. First, what they call Open Innovation, in which they analyse the external ecosystem, dedicating funds to research into the other companies and Start-ups in the marketplace. And secondly, Internal Innovation, where resources are used for a more specific review of company assets distributed worldwide, with the aim of evolving and upgrading them. They also adopt measures in an attempt to promote Digital Certification for all their employees, and have in place longer-term projects to research the possible disruptive technologies expected to emerge over the coming years. For Martín Villa, there are three important aspects on which goals should be focused: the need to make more of Artificial Intelligence, which is no longer an abstract term but is increasingly embedded in business processes, the growing importance of investment in security or the protection of digital assets to mitigate risks, and the desirability of effective application of Blockchain technology, focusing it on essential business procedures, as an assembler for processes that require optimal use of data. The world is rapidly changing; companies need to know exactly what consumers’ demands are at any given moment, so as immediately to offer them products and services that meet their expectations, and they also want to be the first to do so, in order to add the greatest possible value to their margins. However, in the digital world one concept must be clearly established: there are no definitive products. No innovation brought to market, whether by a company itself or by the competition, is perfect, and will in the future inevitably be improved.

**POST-MORTEM ANALYSES**

Being a pioneer in the creation of something new is a thrilling process, although starting out from scratch, without the necessary experience, means properly dealing with our mistakes. We cannot be paralysed by the fear of failure, but need to fail so as to learn, and of course to understand the source of our errors, so as to apply the lessons learnt to future projects. Post-mortem analyses of businesses are vital in order to capture the necessary knowledge. Things should first be tried out on a small scale, as prototypes, which is how Start-ups operate, by measuring the metrics effectively from the outset, examining what works and what doesn’t.
Management have to be convinced of the need to take a step-by-step approach and to progress gradually, before embarking on major disruptive projects. Patience is always advisable in this type of situation.

To develop new innovative practices the process has to begin by calling on employees to submit their proposals for improvement, focused at all times on generating significant benefits for the business. Once these ideas have been received, they are filtered, analysed, and the best of them are selected so as to decide which projects should be initiated. For three months after the prototype is launched, we evaluate how it functions by using KPIs (Key Performance Indicators). These indicators are calculated by means of various parameters, such as customer usage during a particular time period. The tracking of these measurements leads on to the decision as to which projects are shut down and which remain in progress, reassigning employees from the discarded projects to those that are maintained, and performing a subsequent analysis to gain feedback as to the reasons behind the failure of those that did not prove successful.

**TOP MANAGEMENT**

In the opinion of Telefónica’s CIO, in order for positive results to be achieved in this field, absolute support and commitment is required from Top Management, combined with the active cooperation of Internal Auditing, from the outset of the projects. Everyone also needs to be involved in order to ensure precise Risk Management, appropriate legal and regulatory compliance, and to evaluate the possible liabilities that could arise when creating something new. Other vital aspects to be taken into account are the importance of an exact understanding of what is being done, actively listening to all parties involved and identifying the reason for any bottlenecks that might exist between the different areas of the company that could hamper or prevent cooperation among the various departments. Flexibility will become an absolutely essential element in facing the future. Technological changes suggest there will be a shift in the physical location of workers, which will allow tasks to be performed anywhere, and at any time. The inclusion of diversity will also be significant in increasing the role of women at organisations, and employees joining companies will increasingly demand more training and development opportunities.

Progress is being made in achieving an appropriate work-life balance, which will ultimately improve employee performance. In short, we need to plan well for the future, with a mindset of continuous improvement based on trying out new things, effectively measuring how the projects undertaken evolve, and learning from any mistakes that might occur along the way. If you don’t let your business grow, you will kill it. The view of a company as something static or established can have disastrous consequences. The flexibility to adapt and the patience to know how to evolve at the right pace become two fundamental values. In order to create his culture of innovation, which, it should be recalled, must involve all employees irrespective of their role, cooperation and partnership among all areas of the company are essential.

* Summary prepared by Fernando García Zapico
SPONSORS

PLATINUM SPONSORS

SILVER SPONSORS
GOLD SPONSORS

BRONZE SPONSORS
Until recently, the need and expectation for innovation in Internal Audit has not been particularly high. Nowadays, Internal Auditors, their Boards and senior stakeholders recognize that the Function must evolve in order to meet higher expectations over a disruptive and constantly changing business environment. Hence, the need to change is clear. The time for change is now. Question is how we take more forward-looking approaches and increase the assurance coverage with a more efficient use of current resources. Not an easy question...Looking for the answer, our team started a pilot over a range of initiatives to evolve the Function at Sanitas – part of Bupa. We named it ‘Our innovation plan’. The need for achieving more relevant and impactful insights was our target. We aimed to ensure that new audit approaches resulted in relevant and timely—even real-time—advice and insights over significant key business risks. In this journey, the team quickly identified the need and importance to ensure Global Internal Audit priorities are truly aligned to business goals and strategy for achieving those goals. Not only because of the importance of developing a common business language and aligned list of priorities, but also to understand the Internal Audit Function as a ‘True Business Partner’. As you all know, ‘Business Partner’ definition sounds very attractive, how do we make it real? Internal Audit, as third line of defense, is an Independent function. But this does not mean to be isolated. While Internal Audit must preserve its independence and objectivity, we need to take Innovation with the primary goal of improving our own processes to understand and meet stakeholders’ needs – processes that remain under our control. Hence, Bupa Internal Audit operates with coordination and alignment with both corporate strategy and business objectives while maintaining their independence. As a true partner we help Bupa clients to live longer, healthier and happier lives. ‘TRUE BUSINESS PARTNER’

According to our experience, being a ‘true business partner’ while applying ‘innovation’ might sound like complex terminology.
For some of you, Innovation might evoke complex technology or well advanced data analysis techniques. For our Internal Audit Group Innovation in internal audit is not rocket science and means the tools & approach to unlock our potential and provide effective assurance in a disruptive and continually evolving business environment.

However, this is our own definition and you should seek your own while looking for initiatives to maximize your value.

We are showing our approach to innovation and hopefully you will find some synergies or ideas that might be applied in your part of the world. There are thousands of ways of being Business Partner while you keep your independency and apply an innovative approach. We are simply sharing a rage of practices we use in order to improve our internal and external branding as well as the value we provide to our stakeholders.

**SWOT ANALYSIS**

Our starting point to innovate was a comprehensive analysis to improve our knowledge about ourselves, our stakeholders, and our organizational culture. We performed a SWOT analysis to identify the strengths, weaknesses, opportunities and threats to fix the adequate starting point in our innovation journey.

After the analysis, we identified our priorities focused on being more agile or adaptive to the complex business environment. Stakeholders need more from the Function, forward looking assurance and higher risk coverage while partnering with the Function to widespread the adequate risk and control culture. Our influence, impact and reporting skills were a must and a priority to our internal auditors. Let’s explore some examples of the referred principles:

- **Agile.** Using a close and continuous monitoring type audit we have developed an agile framework to provide assurance over transformational initiatives and significant projects. We meet the expectations and provide higher risk coverage on a more real-time basis. The approach includes attending, observing and providing input at relevant working groups and governance forums, reviewing and challenging outputs and providing observations and insights for management consideration where issues or emerging risks are identified.

Close and continuous monitoring helps to action management remediation plans as the project/issue/initiative is on-going and internal audit contribute to promoting risk and control culture.

- **Influence.** We have defined an Influence Map considering the most significant stakeholders for the Internal Audit function. This map enables the definition of effective communication initiatives depending on the target levels and we ensure the Team is accountable to provide key insightful messages at their levels.

Stakeholder Journey. We have performed a comprehensive analysis over the internal audit activity cycle and its relation with stakeholder’s satisfaction. The purpose was identifying the activities, more critical during every audit project, to analyze what can go wrong and anticipate our approach to provide higher value and maximize stakeholders’ satisfaction throughout while meeting their expectations.

- **New ways of communication** and video report. To become a business partner aligned with our stakeholders priorities we invest in Auditor’s communication skills. But not only in writing, we also really appreciate the idea of using technology to communicate our messages in more innovative ways to spread our observations and messages to the whole company.

We have developed an audit report in video format using technology to share our opinion and insights. The video report is a no longer than 2 minutes and includes the most important messages obtained from the audit engagement. The video report is a supplement of the written report.

As you may be aware, Innovation at Bupa Internal Audit is the starting point to think in the Internal Audit Function of the Future. According to our experience, this is a long-term journey for which it is important to be focused on:

- **Listening to your own Organization music.** You need to understand the strategy and the initiatives of your part of the work, business and understand the innovation within its environment.

- **Know yourself.** Know your stakeholders. You need to identify your Function strengths but also to see the threats as opportunities to evolve. This will allow you to define initiatives focused on key priorities for your own internal audit processes.

- **Innovation is not difficult.** Open brainstorming with your Team could be a good starting point to identify good innovative activities to initiate your innovation program.

- **Design your own “suit” to evolve.** Sadly, we do not have a magical formula to share with you when we speak about innovation. We really know our initiatives works for us but this does not mean that they will work for everyone. You might need to tailor your innovation strategy according to your Internal Audit Function.
On coming in to Novartis as Head of Internal Audit in 2010 – I left in June 2018 and write here in a personal capacity - I grappled with the questions of how to position the function in the organization. Was it right for it to be the ‘policeman’ as it traditionally had been (as in many other organizations)? How, with my business experience, could I make internal audit more relevant and bring value to the organization? Novartis was in 2010 and still is a massive organization, with major financial dimensions and a wide variety of activities. Fortunately, Novartis has a large internal audit function that has enjoyed a lot of support from the board and management over the years. Novartis also has high ambitions and, working in life sciences, it needs to operate sustainably in a highly regulated environment. So auditors need to provide assurance on many requirements. The business is also highly innovative and Novartis aims to become a trusted leader, so assurance is also needed on innovation and emerging risks.

THE ‘POLICEMAN’ AND THE ‘DOCTOR’ APPROACH

In these circumstances, which auditing approach is better, the reactive (‘policeman’) approach or the preventive (‘doctor’) approach? The ‘policeman’ approach takes the company rulebook as its basis, and is about enforcing the rules, arresting (and eventually punishing) those who break them, and thereby protecting the organization. One of its merits as a model is that it is intuitively understood and widely accepted: most non-auditors expect auditors to act somewhat as policemen.

The ‘doctor’ approach aims to provide a holistic diagnosis with the purpose of curing the patient rather than judging them. It requires a lot of skill and judgment: checklists are not enough. The wider organization also needs to be receptive: internal audit needs to appeal to the self-interest of management that their part of the organization be well-diagnosed and treated, and management need to be willing to put the ‘policeman’ image to one side. Good collaboration is essential: the doctor’s diagnosis benefits if the patient freely describes their symptoms and background factors in their life and family.

While appealing, the ‘doctor’ approach to auditing does have shortcomings. The audit conclusions are more judgmental and therefore more debatable, and this may lead to long, drawn out discussions that contribute little to organizational improvement and may put strain on relationships. It is harder for the auditors to stand their ground than judging them. It requires a lot of skill and judgment: checklists are not enough. The wider organization also needs to be receptive: internal audit needs to appeal to the self-interest of management that their part of the organization be well-diagnosed and treated, and management need to be willing to put the ‘policeman’ image to one side. Good collaboration is essential: the doctor’s diagnosis benefits if the patient freely describes their symptoms and background factors in their life and family.

While appealing, the ‘doctor’ approach to auditing does have shortcomings. The audit conclusions are more judgmental and therefore more debatable, and this may lead to long, drawn out discussions that contribute little to organizational improvement and may put strain on relationships. It is harder for the auditors to stand their ground than judging them. It requires a lot of skill and judgment: checklists are not enough. The wider organization also needs to be receptive: internal audit needs to appeal to the self-interest of management that their part of the organization be well-diagnosed and treated, and management need to be willing to put the ‘policeman’ image to one side. Good collaboration is essential: the doctor’s diagnosis benefits if the patient freely describes their symptoms and background factors in their life and family.

While appealing, the ‘doctor’ approach to auditing does have shortcomings. The audit conclusions are more judgmental and therefore more debatable, and this may lead to long, drawn out discussions that contribute little to organizational improvement and may put strain on relationships. It is harder for the auditors to stand their ground than judging them. It requires a lot of skill and judgment: checklists are not enough. The wider organization also needs to be receptive: internal audit needs to appeal to the self-interest of management that their part of the organization be well-diagnosed and treated, and management need to be willing to put the ‘policeman’ image to one side. Good collaboration is essential: the doctor’s diagnosis benefits if the patient freely describes their symptoms and background factors in their life and family.
in discussions with the auditees, because there is no clear rulebook as reference.

Used well, however, the ‘doctor’ approach can be very successful in bringing timely insight into potential problems in the organization, promoting risk awareness and prompting corrective action before risk materializes.

My experience over time has led me to believe that choosing the ‘policeman’ or ‘doctor’ approach is more a question of circumstances and context than of intrinsic merits.

In industries such as pharmaceuticals and banking, where there are strict regulations, heavy fines and reputational consequences, the ‘policeman’ approach is to some extent inevitable: after all, those leading the organization must know whether people are following the rules and must take quick and decisive action if they are not.

When the regulated area is unfamiliar or the regulations are changing, auditors need to exercise care: the organization itself may still be learning the rules, the auditors also need to gain confidence that they understand them.

There may also be value in assessing the roll-out and change management of the new regulations: this part is typically better done with a ‘doctor’ approach.

So sometimes in auditing regulated areas a combination ‘policeman’ and ‘doctor’ approach is needed and this is complex to manage.

In pharmaceuticals and banking, however, there are areas of activity that are less subject to strict external or internal regulations. In these cases, a ‘doctor’ approach is in my experience more likely to add value.

The auditor needs to be knowledgeable, professional and good at influencing without authority, while the organization also needs to be both receptive and cooperative: the ‘doctor’ approach is not necessarily the easier option.

As a proponent of risk-based internal auditing I believe both the ‘policeman’ and the ‘doctor’ approaches play an important part.

The quotation below comes from the excellent guidance in risk based auditing provided by the Chartered Institute of Internal Auditors (UK and Ireland).

The italics highlight where, in my view, ‘policeman’ approach can add value, and the bold type where a ‘doctor’ approach can add value.

Both separately and in combination they can help to make risk-based internal auditing real and value-adding:

“Risk-based internal auditing helps to provide the board with assurance it needs on three areas:
1. Risk management processes, both their design and how well they are working
2. Management of those risks classified as ‘key’, including the effectiveness of controls and other responses to them
3. Complete, accurate and appropriate reporting and classification of risks”

CONCLUSION

In conclusion, both reactive (‘policeman’) and preventive (‘doctor’) audit approaches have their place and uses, both separately and in combination, overall supporting risk-based internal auditing in any organization.

The key learnings are:

- It is important to recognize when an audit topic is in a regulated or unregulated area, and tailor the approach accordingly. Auditing in a regulated area will always need at least in part the ‘policeman’ approach because of the need to check whether the rules and being followed and ensure prompt resolution if they are not.
- Both the ‘policeman’ and ‘doctor’ audit approaches require skills and knowledge, the ‘doctor’ approach especially because of the amount of judgment required.
- It is important to engage and communicate with the organization as a whole, in particular with the auditees, so that internal audit’s work is understood and its value recognized.

The wider organization also needs to be receptive: internal audit needs to appeal to the self-interest of management that their part of the organization be well-diagnosed and treated, and management need to be willing to put the ‘policeman’ image to one side. Good collaboration is essential: the doctor’s diagnosis benefits if the patient freely describes their symptoms and background factors in their life and family.
Since the appearance of the term Big Data, one of the most common ways to define these kinds of technology and related projects has been by means of the so-called V’s. Typically, a big data project is based on large datasets (Volume), involving many different data origins (Variety), with real-time very fast data (Velocity), for solving a concrete business problem (Value) and dealing all the issues of reliability data may suffer (Veracity).

This last point is the one we want to focus on: organizations are making data-driven strategic and tactical decisions as well as designing new services and products for changing the experience of their customers relying on their data so this information must be trustworthy. To this end, organizations must continuously validate the quality of their data, as well as the processes involved in data gathering.

**Why may data be unreliable?**

Imagine your company has a data repository, composed of different tables, containing perfectly structured information, that is, we do not find apparently wrong data within the fields of these tables. However, your data may be not directly exploitable because these values contained in the tables are not veracious.

For instance, many industrial companies are setting up sensors in their manufacturing plants for monitoring workers presence or recording temperature and vibrations of different components to predict when a maintenance task is needed. However, each of these physical measures has an error simply because of the nature of the device.

When we analyse this data, if we do not consider we have a measurement error inherent to the physical nature of the sensor, we may be led to the wrong conclusions. This is something we can see every day on our mobile phone: when we launch an app to get the best way to reach a place, at the beginning and in some places like tunnels, these apps are not able to locate us perfectly, and, typically, a circle around our estimated position is plotted. If we are some of these companies and we are saving data to analyse mobility patterns, we should also save the error circle so that this information may be also used in future projects.

A different kind of possible source of unreliable data comes from user declarative information. Imagine your company has a digital platform where users must declare their age in order to use the services you are providing and only people who are at least 18 years old are allowed to use them. If you are only requesting from a user a declaration of age with no further validation, users may lie.
and then under-age people will be able to use services they are not allowed to. The key point in this case is the process: our company is not ensuring the conditions for the usage of the service because we are not doing any validation of the data we are collecting. Processes must be redesigned to assess the quality and veracity of the data provided by the user. This is a critical issue for both operational and analytical reasons: if data is not reliable, any conclusion that may be extracted will no longer be valid.

Lastly, time is also crucial in data quality. Many data sources do not change in time: for instance, if we register a transaction made by a customer, this information is not going to change in the future, it has been recorded and there is no process to modify it. However, other information may change and our data will not reflect these modifications if we do nothing to solve this. Imagine you are a business-to-business company and within your CRM tool you save information about your potential customers and the key person you should contact to present your services and products. Typically, information such as the full name of your contact, his/her phone number or the position in the company. But this information is not static: people change their phone number, move to different positions inside a company or they also may move to a different company. As a consequence, when one of these events occurs, our information becomes automatically obsolete and, despite it being perfectly structured and apparently valid, it is no longer trustworthy in terms of analysis.

**TRUST THE PROCESS**

Every one of these issues we may find related to data quality can only be solved if we are able not only to gather information but also govern both data and processes successfully. Companies are changing the way they organize information and are creating positions inside the company responsible for managing data and processes. Currently two new roles are emerging:

- **Chief Data Officer**: person who is responsible for deciding the data sources to ingest and monitor in the information repository, managing the processes involved in the data ingestion process or security of the information (access, anonymization, availability of the information ...). This role will design the technological information architecture and will provide service to all the analytical teams in the company.

- **Chief Information Officer**: the main data user and consumer inside the company, responsible for solving the analytical requests in the organization, analytical work efficiency and reusing, designing data science roadmap and creating the teams for providing information services for each department in the company.

Setting teams for managing all the data complexity and for exploiting the information from the point of view of business will also allow the organizations to create trustworthy processes and make the company proud of its data. And this is the fundamental point: many companies invest huge quantities of money in organizing their data, in creating big infrastructures to build analytical data repositories but the key is all the company should trust the quality of the data. Otherwise, we will find familiar situations: there are silos of information between different companies, there is no common view on how to extract all the value from information and we will find every department managing their information without any collaboration between them. This is why companies must trust data processes.
To meet the needs of the Internal Audit Functions and their stakeholders, a task force of internal auditors developed the Internal Audit Ambition Model (IA AM). The IA AM was introduced at the IIA Netherlands Conference in June 2016 as a self-assessment tool. Users were enthusiastic and provided us with useful comments for further improvement. In 2017, it developed into a communication and benchmarking instrument. It supports Internal Audit Functions in getting up to standard with the IPPF and setting their ambition level. In the meantime, auditors from 20 different countries had also read our booklet and contacted us in order to receive the model. That was an unexpected success! With the launch of the IA AM at the ECIIA in Madrid on 4th October 2018, we will have reached a new milestone.

We want to share our experiences with all the members of IIA Global. The ambition model was a game changer for our professional association in the Netherlands. Several Internal Audit Functions have been using the model as a strategy and team building activity. By examining the current state of their Internal Audit Functions and discussing the scoping and ambitions, the teams experienced a greater-shared vision of the future of their Internal Audit Functions. Some Chief Audit Executives (CAE) also discussed the area with the Audit Committee.

WHAT IS THE AIM OF USING THE IA AM?

The ambition model has five levels to define your current and ambition level. It contains concrete, good practices that give the CAE guidance and inspiration when he/she aims for the audit services to go beyond compliance with the IPPF. The model supports the CAE formulating strategic objectives, evaluating the current level of the Internal Audit Functions and defining a roadmap to achieve the stated objectives. Furthermore, the spider web/dashboard can help in the dialogue with the Audit Committee and/or Supervisory Board to determine which aspects should be taken into account when assessing the internal audit mandate and ambitions. We aim for the following three objectives:

- For CAEs: Dare to express your ambitions and check if you comply with the IPPF standards. The IA AM supports the development of a clear roadmap to realize your ambitions and it is an easy tool to compare
your ambition and achievements with your peers.

- For board members: The IA AM supports your dialogue with the CAE in a clear and simple way by providing you with the relevant themes and topics.
- For professional bodies: Use the IA AM as a benchmark tool to gain insight into the current state and ambition levels of Internal Audit Functions in your country. Encourage the sharing of good practices through meetings/round tables/publications. Set up a coaching or mentor program for CAEs and their internal auditors to at least get up to standard with IPPF.

Our aim is to substantively enhance the practice of the internal auditing profession and to challenge colleagues around the world to continue on their way to further professionalization.

**IA AM IN A BRIEF OVERVIEW**

The IA AM consists of the following three columns which are explained below:

1. Themes: Six themes are identified for an IA activity.
2. Subthemes and topics: To further detail and clarify the specific aspects that should be addressed by the Internal Audit Functions in order to progress to the next ambition level; the six themes have been divided into eleven sub-themes and thirty-eight topics.
3. Essential activities: The activities to be performed, are defined as essential activities for each of the topics. In order to measure and rank the topics, essential activities are identified for each of the five levels of the Ambition Model.

In addition, the levels illustrate the stages through which an Internal Audit Functions can evolve as it defines, implements, measures, controls and improves its processes and practices to meet its ambitions. The outcome of the IA AM questionnaire results in a spider web (dashboard) that enables high level communication with the executive and supervisory board and other stakeholders. In the spider web the blue line shows the level achieved. The orange dotted line is the desired ambition level which is set by the CAE/Internal Audit Functions. Based on our experience, level 3 should give you an indication on compliance with the IPPF standards, but of course, a final assessment as to whether an Internal Audit Functions generally complies with the IPPF is to be determined via an External Quality Review performed by the professional body in your country.

This dashboard above reflects the results of the 2017 benchmark and gives an initial insight into the current state and ambition levels of the Internal Audit Functions in the Netherlands, in this demanding environment. Given the relatively small number of benchmark participants, it was too early to conclude that the results were statistically representative of the internal audit profession in the Netherlands. However, during the discussion of the results in the CAE Forum, this initial insight was acknowledged. Let’s take a step into a broad, professional dialogue amongst auditors by sharing experiences, insights and good practices. Be the game changer. Use the IA AM!

Are you curious about the achieved level of your Internal Audit Functions and are you willing and ready to set your ambition level by using the IA AM? The model is free of charge. It is only your feedback, which we strongly encourage you to send us, that will enable us to regularly further develop and improve the model.

The ambition model was a game changer for our professional association in the Netherlands. Several Internal Audit Functions have been using the model as a strategy and team building activity.
For Campari, which currently occupies sixth place on the spirits industry ranking with 50 brands sold around the world (190 markets), the management and control of social risks has become a fundamental part of its strategy. Social media networks are having a radical impact on our traditional world. Real-time access to user-generated content allows people and companies to make use of innovative channels capable of accelerating connections and streamlining cooperation. As citizens of our time, we must be a part of this evolution and therefore make an effort to live this large-scale change.

It is essential to understand that our confidence in technology and the current digital revolution mean we need to update the concerns and risks of five years ago because there is a genuine chance they have become obsolete. This change means that the greatest risks to which a company like Campari is exposed include reputational risk, compliance with new privacy rules (GDPR) and those tied to brand safety in terms of knowing where and how your advertisements appear. We currently live in a digital and social media era, in which such applications as Facebook, LinkedIn and YouTube form part of our daily lives but only represent the tip of the iceberg. Social media broaden the reputational risk spectrum and can lead to consequences that affect corporate levels. They therefore need to be taken into consideration and analysed for correct management of the risk. It is important to understand that the digital revolution and social media networks are changing the ground rules because, among other things, the customer journey or user relationship model has been redefined from one in which they are passive receivers where communication took place in one direction (one-way) and channel to one in which they are active users who act as both receivers and transmitters through multiple channels where they share their feelings and opinions on the various messages and campaigns received (multi-interaction).

**NEW PLAYERS**

New players are therefore emerging, such as influencers, who are capable of using their posts on social media networks and millions of followers to not only impact brand image and reputation but, in some cases, also impact company share values. This aspect poses one of the greatest risks from social media as it complicates the calculation of potential impact and repercussions from every individual action on social media. This is why, in some cases, influencers can be categorised as external risks. This phenomenon is being approached by Campari from a different angle based, among other things, on questions aimed at assessing how real the follower numbers quoted by said influencers are and therefore analysing how to try to measure and predict both the positive and negative impact of their posts on social media. Any action, including unintentional action, can lead to negative effects on social media. Based on experience, incidents
and their repercussions on social media pass through various stages: growth, development and explosion until they eventually fade away. However, we should bear in mind that one of the main characteristics of social media lies in that nothing is forgotten and that all the content generated in the past (good or bad) will be accessible forever. Furthermore, it is a fact that social media have complicated the management of privacy not only due to the technological evolution of Cloud computing and the decentralisation of processes and data but also due to the need to comply with new regulations on data protection and confidentiality assurance (General Data Protection Regulation).

The incorrect or incomplete management of privacy can lead to repercussions on both brand image and economic penalties. This might include the publication of a selfie during an event on a Facebook wall. As internal auditors, we are expected to be trained in detecting, managing and avoiding the key risks stemming from this evolution, as well as be prepared to support the company in implementing the right internal control system.

**MANAGEMENT OF SOCIAL RISKS**

Based on its experience, one possible approach to the correct management of social risks is underpinned by the following four pillars:

● Strategy updates, incorporating the new digital risks into the strategy, accepting the complexity of the digital environment and therefore assuming that it is almost impossible to control the risk entirely.

● Drawing up a road map for implementation of the strategy, in which the new roles and responsibilities associated with the digital environment are defined (such as the community manager), new governance requirements are defined and implemented for marketing agencies, and control measures are defined and implemented for the content exchanged between marketers and agencies.

● Training and awareness, for both internal and external staff because sharing a common language in this new environment is key, and for focusing company efforts on brand reputation and producing a single interpretation of the brand safety concept.

● Improved controls, ensuring both compliance with internal policies (e.g. defining and implementing desired combinations between page content and the brand, avoiding undesired combinations such as advertising on websites with adult content, violence, etc.) and existing regulations (e.g. data protection and privacy); as well as using mechanisms, applications and third parties that always seek to protect brand image. Nonetheless, it should be taken into consideration that it is impossible to cover the entire social media spectrum and therefore provide full assurance on social risk mitigation.

*Summary prepared by Javier García Núñez*
I have spent a significant amount of time in my career dealing with Audit Committees. As a Chief Audit Executive, I provided many different Audit Committees with numerous reports, recommendations, opinions and of course independent assurance. More recently I have served on Audit Committees as a non-executive member and have been on the receiving end of Internal Audit’s information and advice. These Committees have been in both the public and private sectors, including very large organizations such as HMRC, the UK’s tax collection department and Lloyds Bank. My various associations with Audit Committees have given me an excellent insight into what they need to do to be effective. Without doubt, the most effective Audit Committees that I have worked with all had one thing in common. They enjoyed an excellent working relationship with Internal Audit. How was this achieved? I hope this article will shed some light on this.

Audit Committees are set up by the Board (or its public sector equivalent) and their members are non-executive directors. In the UK Private Sector, the Audit Committee acts independently of executive management to ensure that shareholders’ interests are properly protected in relation to risk management, internal control and financial reporting. In the UK Public Sector, the Committee provides independent assurance on the adequacy and effectiveness of the organization’s risk management framework, internal control environment and the integrity of the governance and financial reporting processes.

AUDIT COMMITTEE

The Audit Committee is very important because, whilst the Board is ultimately responsible for governance, the Audit Committee can provide it with significant assistance and support by providing challenge, assurance, advice and oversight.

How does Internal Audit fit in?

As the only truly independent provider of assurance, Internal Audit is a very important supplier to the Audit Committee and it is imperative that there is a good working relationship between the two. The Audit Committee and Internal Audit are closely connected in a number of ways. The Audit Committee assesses and approves the IA Charter; ensures Internal Audit independence, i.e. reporting line independent of the executive; monitors the quality and effectiveness of IA work; assesses IA resourcing; evaluates and approves the ‘risk-based’ IA Plan; ensures the collective assurance roles are coordinated and optimized; assesses IA report findings and monitors...
management’s response to IA findings. Audit Committees should be able to rely on Internal Audit to provide independent assurance over the controls in place to manage risks and to provide fresh, different and independent perspectives on issues that really matter. As a non-executive member of the Audit Committee, I do not have a team around me so it is difficult for me to know what is going on in the organization. I need help. I hope that my internal auditors can give me this.

In return, I can ensure that Internal Audit is independent, listened to, and has sufficient status to be a key influencer. I also believe that I, and my Audit Committee colleagues can help to create a culture of challenge and transparency in the organization enabling IA to report freely, with candor and without fear of retribution.

I have high expectations of Internal Audit. Of course I expect it to be professional and to work in accordance with professional standards. I expect internal auditors to be qualified or studying to be so. But technical proficiency is not enough!

I want my internal auditors to have a good knowledge of the organization, to have their ‘finger on the pulse’ and know what is going on. I want them to speak up when necessary and to provide early warnings where there are significant risk exposures.

I WANT, I WANT...

Above all, I want them to be a positive influence and to help the organization be successful. I want them to be forward looking and to be involved when key decisions are made, such as on steering groups for major change initiatives and other important committees. I want them to contribute to the organization’s success by promoting best practice and by using their expertise, not just to highlight problems but to recommend solutions.

I also want to see that internal audit is taken seriously by the business and effectively influences management to take improvement action. Above all, I want a truly independent view, not influenced by executive management.

Whilst I am clear on my expectations of Internal Audit, are these expectations always met? The answer is, not always. Some internal audit teams have never tried to find out what the Audit Committee wants but have just audited what they were able to do. They have sometimes had capability gaps, e.g. ability to audit complex IT systems. Sometimes they have not evolved in line with changing business demands and technological advancements. In the main, internal audit teams have been technically proficient but not all have had sufficient influence.

So what would my advice be to CAEs? Firstly, try and understand the Audit Committee’s requirement for assurance and strengthen alignment with other ‘Lines of Defense’. Continually ask for feedback from the Audit Committee. Develop a shared understanding of risk and governance concerns. Provide quality assurance, challenge and advice. Help the organization achieve its goals – always bear this in mind. Be involved, proactive, knowledgeable, constructive and challenging. Focus internal audit activity on key risks. Adapt to the changing risk landscape. Share, communicate and champion best practice. Up skill to meet changing demands and harness the power of technology. As a member of the Audit Committee, there are a number of questions that I always ask myself. Is internal audit making a positive difference? Do we believe and trust what it tells us? Are its findings relevant, proportionate and clearly evidenced? Do business units want internal audit involved. Is it represented on major governance forums and major change programmes? Last but not least, are we paying the right amount for this assurance?

CONCLUSION

In conclusion, I believe that Audit Committees make a key contribution to effective corporate governance. The relationship between Internal Audit and the Audit Committee is vitally important and requires significant effort and investment in time to build and maintain. Internal Audit will only prosper if it understands what the Audit Committee expects it to do and must be a dynamic force able to adapt/improve and deliver in line with changing expectations.
It is common to relate the word neuron with the human body, with the brain, with the marrow. After all, that word represents those cells that compose the nervous system, whose function is to pass information instantly to each other. But in a world where Artificial Intelligence is the order of the day, how could there not be digital wisdom from the hand of artificial neurons? As could be expected, their name is not by chance, the Artificial Neural Networks or ANN are computational models that are inspired by the neurons from the nervous system, not only in their physical aspect but also, they perform a very similar task to brain neurons. If you haven’t been able to attend this lecture at the Super Internal Auditors 2018, you might find this article too complex to understand, however, Iván Martín, the speaker encourages the readers and the people interested in it to read it and ask him about any doubt it may lead to. Just as a brain uses a network of interconnected neuron cells to create a massive parallel processor, the artificial neural networks use nodes to solve learning problems. A brain neuron receives signals by the dendrites, that is to say by “the arms”, which in turn determine the importance of the impulse or relative frequency. When these incoming signals accumulate, it reaches a limit and is triggered through an electrochemical process in the axon, also known as “the body”. At the terminals of the axons, the electrical signal is processed again as a chemical signal that is passed on to neighboring neurons through a small space known as a synapse. And so, it continues successively.

**THE HUMAN BRAIN**

The human brain is made up of 85 billion neurons, which results in a network capable of representing a huge amount of knowledge. A cat has a billion, a mouse has 75 million and finally a cockroach has just one million neurons. In contrast, as is to be predicted, neural networks remain small in comparison, reaching only a several hundred, which - breathe deeply - makes it impossible to create an artificial brain in the future.

Product of Machine Learning, these neurons were born in 1958 under the name of Perceptron, the first artificial neural network. But it was not until 2012, when another historical network was born, called the Deep Neural Network, developed by the GoogleBrain project to recognize images and texts and detect patterns. That is its main function; these machine learning models are able to detect the most complex patterns in large amounts of data. That is why they have gained popularity throughout the years, while their advances continued to spread through the fields of Computer Vision, text processing and voice recognition. However, the way neural networks work and function must be demystified in order to learn from them and be able to adjust them to predict the desired result, which...
can be applied to any sector and to its specific challenges. Its functions can be specified in three different categories: activation function, a topology network and a training algorithm.

**THE ACTIVATION FUNCTION**

First things first, the activation function is the mechanism by which the artificial neuron processes the incoming information and passes it through the network. In the case of biological neurons, the activation function could be imagined as a process that involves adding the total input signal and determining if it meets the activation threshold. If so, the neuron passes the signal; otherwise, it does nothing. In terms of Artificial Neural Networks, this is known as a threshold activation function, since it results in an output signal only once a specific input threshold has been reached. On the other hand, the capacity of a neural network to learn is rooted in its topology, or in the patterns and structures of interconnected neurons. In general, the largest and most complex networks are those that are most likely to be able to identify more subtle patterns and complex decision boundaries. However, the power of a network is not only based on the size of the network, but also the way in which the units are arranged.

**THE TOPOLOGY OF THE NETWORK**

Finally, the topology of the network is a blank slate that, by itself, has not learned anything. It is like a newborn child, who must be trained with experience. As the neural network processes input data, the connections between neurons are strengthened or weakened, similar to how a baby’s brain develops as he or she experiences the environment. The connection weights of the network are adjusted to reflect the observed patterns over time. Training a neural network by adjusting the connection weights is highly computational. The algorithm, which uses a backward propagation error strategy, is now known simply as backward propagation.

A practical example of its operation is the Optical Recognition, or as a network of artificial neurons, they achieved a base of training, corrections and later improvements to create an algorithm that would identify handwritten numbers on paper. As well as another related to the Classification and Regression, such as calculating the strength of a cement of foreign origin taking into account other cases with similar characteristics.

In conclusion, it can be adapted to the creation of numerical patterns such as Classification and Regression, besides having the ability to model in a more complex way than any other algorithm patterns. However, it is an intense and complex process, leading to the overheating of the data from the training received.

Iván Martín Maseda was the speaker who presented this new issue during the Super Internal Auditors 2018 held in Madrid on October 4. His experience as the Academic Director of the Data Sciences Bootcamp at IE Business School, along with his position as Chief Technology Officer at the Spanish Startup Binfluencer means working with Artificial Intelligence on a daily basis and therefore he is the most appropriate speaker.
Identifying wrongdoing, misconduct or fraud is the first step. However, disclosing such observations appears to be a challenging second step. The main barriers individuals experience is i) the fear of possible adverse consequences (professionally, privately) by reporting such cases as well ii) their concern that insufficient/no action would be taken. Whistleblowing” is the commonly used term when an individual discloses reports wrongdoing. At HEINEKEN another term is used instead: “Speak UP!” Given the more positive connotation of this terminology, we believe it proactively encourages employees as well as third parties (suppliers, customers, consumers) to express their observations. A strong speak up framework takes into account the elements of culture, protection, procedures as well as continuous efforts to keep it alive. In particular:

1. CULTURE - Create a safe environment for speaking up
   ● The foundation lies in the commitment from top management to take ownership of the speak up process.
   ● Fostering a safe environment starts with creating and maintaining awareness of the process amongst all employees.
   ● Multiple communication tools and campaigns (e.g. homepage, internal communication tools, newsletters, and posters) may be applied to achieve this.
   ● Mandatory trainings (e.g. classroom, eLearning, town hall meetings) facilitate a discussion of possible dilemmas as well as clarify the reporting procedure.

2. PROTECTION – Maintain confidentiality and protection of reporters
   ● The confidentiality of reporters must be ensured at all times.
   ● Providing a mechanism/platform to express concerns anonymously increases the likelihood of speak up.
   ● Robust protection of reporters from any form of retaliation as well as by protecting their identity through all stages of the investigation must be the cornerstone of the process.

3. PROCEDURES – Couple reporting channels with effective response systems
   ● Different reporting channels (e.g. telephone hotline, online, in-person reporting) must be available 24/7/365.
   ● To ensure confidentiality such services may be outsourced to third parties.
   ● Establish an effective response system by providing feedback to reporters throughout all stages of the investigation.
   ● A case management system for recording, investigating and monitoring of cases is an important enabler for the speak up process. Responsibilities and accountability need to be clearly assigned.

4. KEEP IT ALIVE
   ● Establishing a speak up process is not a one-off exercise. Periodic refresher campaigns help to maintain the momentum.
   The Board of Directors is responsible for establishing an effective speak up process as part of the Corporate Governance which entails effective risk and control management. As such, this process is strongly linked to the core responsibilities of an Internal Audit function. However, the independence and objectivity of the department must not be compromised.

Internal Audit departments may opt to not be directly involved in the speak up process and rather provide assurance on the effectiveness of the process itself. This includes audit procedures around whistleblowing policies, procedures, culture, management information and third party services. HEINEKEN Global Audit opted to be an indirect part of HEINEKEN’s speak up process by participating in the speak up governance and executing fraud investigations for specific, pre-defined cases. However, the department is not responsible for managing the overall speak up process itself. Through this role the department can contribute to strengthening the internal control environment of the company while – at the same time - maintaining the objectivity and independence of our profession and department.
THE ATMOSPHERE THAT WE HAVE EXPECTED
What is IOTA? The Intra-European Organization of Tax Administrations (IOTA) is an international association with headquarters in Budapest whose members are Tax Administrations of 45 European countries. Founded in 1996 with the purpose of promoting a fiscal modern system in Europe’s Eastern countries, it has evolved towards a wider forum promoting administrative cooperation and best practices exchange, by means of an annual program of multilateral activities (seminars, workshops, conferences, etc.). Over time, one of the most important lines of work, leading to the major achievements, deals with training of Tax Administrations’ employees and the constitution of transnational networks of civil servants with similar tasks in their countries. Recently, the organization also launched the construction of common instruments, especially for information analysis.

Spain, represented by the Spanish Tax Agency (AEAT), was previously an associate member of the organization and joined it as a full member in 2006.

What is the scope of the internal audits?

To improve its governance and exercise an adequate control on the Secretariat, the unit in charge of the ordinary management of the organization, its Chart provides IOTA with an annual internal audit performed by two professionals belonging to the member organizations. The internal auditors are elected by secret voting of the members during the General Assembly and should possess a profile adapted to the function developed in terms of knowledge and experience.

The internal auditors must be independent in their function and submit their final audit report to the Presidency and to the General Assembly, the latter the maximum government body of the organization, which approves it or rejects it. The article thirteen of IOTA’s Chart indicates that the internal auditors must check the processes of the organization, examine its viability and economic efficiency, supervise the internal control system, verify the financial reports and address proposals derived from their analysis, helping thus to mitigate the corporate risks. The internal auditors also carry out a follow-up of the effective compliance with previous audit recommendations, contributing to continuous improvement of the organization.

The IOTA’s General Assembly selected the author to act as one of the internal auditors on two occasions. The working language of IOTA has been English since its foundation; hence, the audits were entirely performed in this language.

How are the internal audits developed?

The internal audit process begins with the concretion of the internal control objectives following an interaction of the auditors with the Executive Council, collegiate body that rules the organization between General Assemblies. The Executive Council is composed of nine countries, selected for an annual mandate during the General Assembly. The Executive Council holds meetings four to six times a year and has the faculty to propose...
specific topics to the auditors, in order to make a general agreement on the annual audit plan. The auditors supervise the internal control system by means of two kinds of activities. Firstly, they examine the relevant documentation of the organization, systematically received from the Secretariat. Secondly, they make two follow-up visits to the IOTA’s headquarters in Budapest. During the first visit, they contact the Secretariat and approach the specific topics of the audits. During the second visit, they assure the reliability of the main financial documents and operational results of the last year, which have been elaborated or compiled by the Secretariat.

The internal auditors document their annual activity in an audit report. Firstly, they submit the draft report to the Secretariat and the Executive Council, following a contradictory process. Finally, they present the latest version in the General Assembly for the approval or rejection by means of voting of the member states.

The auditors can only exercise the mandate consecutively in two occasions. Therefore, the major technical challenge the internal auditors face consists of the maintenance throughout the time of the coherence of the audit function, avoiding omissions and overlaps. This feature, shared by many of the activities that are carried out in an international framework, drives the internal auditors to be particularly scrupulous in the task of documenting their proofs, findings and evidences and, in a natural way, strictly comply with the framework defined in the “International Standards for the Professional Practice of Internal Auditing”.

**EVOLUTION OF THE INTERNAL AUDIT ACTIVITY**

We can distinguish three historical periods since the creation of the IOTA.

The article thirteen of IOTA’s Chart indicates that the internal auditors must check the processes of the organization, examine its viability and economic efficiency, supervise the internal control system, verify the financial reports and address proposals derived from their analysis, helping thus to mitigate the corporate risks.

In the first years, the internal annual audits focused their objectives on the suitable utilization of the budgetary resources, coming mostly from the member contributions. Indeed, in a context of economic transparency, the members’ main concerns were the income and expenditure control and the suitable compliance with the different regulations of IOTA.

In the second phase, of greater maturity of the organization, the audits adopted an approach aligned with the COSO Report and aimed to supervise completely the internal control system. In addition, the internal auditors followed-up the design and the implementation process of the new corporate strategy 2012-2017 and its key points: internal and external communication, especially via Internet, and partnership with broader international entities, such as OECD and EU.

In a third phase, which can be viewed as an “aggregation of value”, the internal auditors act as consultants on topics whose purpose is an effective improvement of the procedures of the whole organization or, specifically, of the Secretariat, besides the accomplishment of the most common and assumed audit tasks. The internal auditors frequently measure the impact of changes. Examples of the latter trend are two studies carried out by the internal auditors on the effective benefits of the Work Program of IOTA and on the efficiency of the communication between the Secretariat and the IOTA correspondents in each member. Another example is the internal auditor’s proposal that routine activities of the Executive Council were handled by written procedures, saving costs and devoting meetings to tasks of more productivity.

**CONCLUSIONS**

In its beginning as an international organization, the function of internal audit was decisive in IOTA to give confidence to the country members and remove any mutual mistrust. Later, the internal audit framework based on international standards, mainly COSO, took over as an adequate instrument to strengthen the internal control system, mitigate risks and increase efficiency. The internal auditors carry out also strategic consultancy at the request of IOTA’s governance bodies. The auditing function also helped the organization to reorient its strategy towards a deeper cooperation between European Tax Administrations and an advanced partnership with other international organizations.

We conclude that IOTA’S internal audit is a success case developed in a very challenging context where public and international features prevail. In general, the case highlights that the internal audit function needs to evolve at least at the same rhythm as the rest of the organization.
Digitalization is not an optional path. It is the ONLY way forward. If the most disruptive technologies like Big Data, The Internet of Things, Artificial Intelligence or Block chain are each already having an individual impact on the insurance sector, imagine when they come together and create a joint impact. This fact is not only pushing the companies to adapt their strategies and the way to see the business they are also transforming their internal processes.

How is the insurance sector facing this movement and concretely MAPFRE? Mainly MAPFRE is focusing on the Client Orientation responding to our customers’ new needs in a dynamic fashion. For MAPFRE Digital Transformation consists of combining Digitization of customer relationships + Digitization of Operations + People from a people centric perspective, while committing to technology as a multiplier.

It applies in the following action lines:

- Client Orientation.
- Excellence in Technical and Operational Management.
- Culture and Human Talent.

**INNOVATION**

We cannot think about Digital Transformation without the concept of Innovation. MAPFRE is not an exception and the Innovation is inside the DNA of the company and its strategy. Starting from a Strategic Plan Based on Digitalization MAPFRE is energizing to be more agile and efficient not only considering Innovation as an internal concept.

MAPFRE has popularized the concept of MAPFRE OPEN INNOVATION (www.insur-sapace.com) where MAPFRE is an additional player of the game collaborating with other companies instead of competing and creating research and work teams to seek short and long-term solutions. Both Digital Transformation and Innovation governed by an Innovation Committee which is totally independent.

How are we living the change in the Internal Audit context?

- Are we adapting ourselves to the change?
- How are we seeing our process right now?
- Are we transforming our service?
- Are we crossing the red line to face this new environment or are we afraid? Do we have doubts when it comes to auditing the context?
- Is this an opportunity or threat?
- What will our position be if we do not adapt our profession to this change?

All these questions have been on our minds for the last two years or so. This situation does not lie in the future, it is with us today. Internal Audit should play an active role in this transformation to always guarantee a controlled environment.

How are we embracing this change in MAPFRE Internal Audit Area?

1. Integration Innovation in the Audit Process. Internal Audit in MAPFRE has always been a pioneer and a reference to impulse different ways to develop the audit activity. However
we think that this spirit has to be organized in a better way to guide the main ideas from our team around the world. For this reason we created an Innovation Process to gather all these ideas together and to integrate Innovation in our daily process. In addition new generations acquire a new relevance in this context. For this reason we decided to test and review our audit process by “other eyes” considering the perspective from a millennial. “Look for a New Internal Audit approach under a Millennial perspective”. This pilot was supported by new methodologies and technics for us (Lean Start-Up, Customer Journey Map, and Design Thinking). The conclusion was very helpful, considering new ideas to transform activities in the audit process and including them in the new audit tool development project (Auditmap).

2. Transforming and acquiring Digital Solutions. Currently Internal Audit in MAPFRE is committed to transforming the portfolio of solutions considering the digital concept as an improvement aspect to facilitate the functionality of our internal and external users as well as to facilitate the efficiency of its tasks.

A clear example is the transformation of our back office solution called Auditmap. From the definition of the new system we are focusing on the simplicity and experience, improving the interaction with internal audit stakeholders. This is not only a technological evolution, this new tool will also enable rich content (including video reports, infographics or any web based content and full online reports).

Internal Audit thinks that reporting is one of the most important activities of our profession and we have to work on improving it. For this reason we have built a new tool (MAPFRE Internal Audit Process BSC) where we offer a landscape for our Management about the business and support processes and their mapping with our audits. We are offering an independent valuation of these processes by country with a degree of coverage based on risks. This is a new view of reporting for the Management of the company from their understanding. Additionally it is important to remark on the importance of our function of Continuous Auditing and Internal Audit Management Indicators, both of which are supported by a BI solution. Continuous Auditing is the collection of audit evidence and indicators in information technology systems, processes, transactions and controls on a frequent or continuous basis throughout a period.

The goals of this function are to:

- Provide more assurance with greater coverage and depth of tests.
- Enhance fraud prevention and detection controls.
- Validate business processes in real-time.
- Improve risk mitigation techniques.
- Reduce internal audit costs.

Finally we have new environments to audit in the Insurance World not included in the Past Audit Universe (Digital Marketing, Price Comparison Sites, Intelligence Automation, etc.). For example in the case of automation process MAPFRE Internal Audit is analyzing during the benefits and kindness of Automation Tools to apply them to improve our audit process. For example we are codifying keyboard entries to interact automatically with legacy systems. This is reducing the time to develop substantive tests to an enormous extent.

3. Updating knowledge and applying new technics (data analytics, design thinking, visual thinking, agility, etc.). In this Digital Ecosystem there are several, not necessarily novel, techniques and methodologies to support this change. MAPFRE Internal Audit is closing its initiatives to improve the Audit Function through them. Examples of these are the Millennials Pilot referred to previously in this article with Design Thinking and Visual Thinking or Lean Method used daily in The Follow-Up Activity Board for improving the Team Organization and Coordination, Balance of the workload, Tasks

Internal Audit thinks that reporting is one of the most important activities of our profession and we have to work on improving it.

Prioritization and improving the visibility of the status of the tasks.

4. Acquiring new profiles. Training to adapt our knowledge to this ecosystem. We cannot meet this challenge to adapt to this change if we are not prepared for it internally. MAPFRE E-CAMPUS is the core of our knowledge, more concretely our Internal Audit University, where we house all training course material and we can expand our knowledge in other subjects. Currently this year we are immersed in amplifying our knowledge in Digital Marketing and Digital Customer Experience. However not all profiles of knowledge are available in our companies right now. For this reason is important not only to prepare our internal resources but also to look at hiring new profiles to enrich our function. Currently this search is focused on Data Analyst.

CONCLUSIONS

We have to embrace the change!!! Otherwise ....We will pass into irrelevance

To achieve this objective:

- We will have to transform our process and sometimes our way of auditing / Preserving our independence but improving our advisory offer.
- Improving our preparation and supporting tools / Acquiring Digital Skills to Understand the Context. Manage the change!!!
- Always working as a team.
- Everybody is important in this context.
- Digitalization and innovation are not options, they are needs.
In April 2015, I had a conference call with my boss, the director of the International Consortium of Investigative Journalists, Gerard Ryle. He didn’t want to tell me the purpose of the call in writing. When we started talking, he spoke to me in code language to avoid naming names. The bottom line was that Süddeutsche Zeitung, a German newspaper with which we had worked in the past, had a leak of about one terabyte, too big for them to handle. They wanted ICIJ’s help, and Gerard was seeking my advice as the editor of the data team on how to proceed.

‘How on earth are we going to do this?’ I thought, but I didn’t tell that to him. Even though I felt a bit overwhelmed by the situation, I knew I had a great team I could count on to tackle this challenge. What I didn’t imagine at that time was how big of a role we, and our technology, would play in what became at the time the largest collaborative investigation in the history of journalism.

The so-called Panama Papers exposed like never before a system that enables crime, corruption and wrongdoing, hidden by secretive offshore companies. It had historic global effects. At least 150 inquiries, audits or investigations were announced in 79 countries around the world due to its revelations. There were resignations from high-ranking officials, including the prime minister of Iceland. The prime minister of Pakistan was removed from office. ICIJ won almost twenty awards, including the Pulitzer Prize and the Data Journalism Award.

We were lucky that such a request for help by Süddeutsche Zeitung came to us at that point in time. ICIJ was founded in 1997 as a global network of investigative journalists who collaborated on in-depth investigative stories but it was not until 2014 that it incorporated a data team for its newsroom. That doesn’t mean data had not been important to investigations before. Data was key in a two-year series on overfishing called Looting the Seas (2010-2012) and also to Skin & Bone (2012), an exposé on the human tissue trade. However, the project where its relevance became more evident was Offshore Leaks (2013).

When Gerard became ICIJ director in the fall of 2011, he brought a hard drive with 260 gigabytes full of documents that exposed the secrecy of the offshore economy. The investigation was not easy on many levels. One of the most difficult parts was making the data available to partners around the world. Seeing that assisting all of them would be too labor intensive, we resorted to technology to help us. We ended up putting the documents in the cloud and making them searchable securely on the web; we had an online forum to share leads and discuss the research, and we created a public website for our readers to explore the names of the people with companies in tax havens. Freelancers – including myself – and the data team at La Nación newspaper in Costa Rica, with which ICIJ collaborated, did most of the data work.

One of the lessons learned from Offshore Leaks –and its sequel, China Leaks– was that ICIJ needed data journalists and programmers in-house. When we started the next project, ICIJ hired two of the developers we had worked with before, Rigoberto Carvajal and Matthew Caruana Galizia, and ICIJ put me in charge of the team. In April 2014, the ICIJ data team was created.

Our first year was hectic. ICIJ published three investigations over that period and a fourth was being reported – many more than the average the organization had been doing in recent years. Our

How Big Data Made World Leaders Resign: The Panama and Paradise Papers

Learn the inside story of these cross-border collaborative projects. The exposes had unprecedented impact with high-level resignations and opened more than 150 investigations in 79 countries.

Mar Cabra
Former Head of Data and Technology at International Consortium of Investigative Journalists (ICIJ)
team’s mission was nothing short of ambitious: ‘to add a data component to every project ICIJ does right from the start and not as an afterthought.’ The projects that took most of our time were those connected to leaks. Our first task was dealing with more than 1,000 image PDFs of secretive tax agreements between corporations and the Luxembourg government. We needed to make them searchable and available to reporters worldwide. It was a similar problem to the one we faced in Offshore Leaks, but this time we wanted to use open-source tools that would allow us to keep improving the system as the need grew. Matthew had the brilliant idea of using a software called Project Blacklight, originally created for library catalogues, to allow reporters to search documents remotely. To improve the virtual newsroom where journalists interacted on a regular basis, Rigoberto proposed to repurpose Oxwall, an open-source social networking software meant for dating – among other things. As we were working on this, the French newspaper, Le Monde, shared with ICIJ 60,000 leaked files from the bank HSBC. They were mostly spreadsheets with names of people connected to accounts in its Swiss subsidiary and the amounts of money in those accounts – in many cases, hidden from the tax authorities. We also used Blacklight and Oxwall in this project and executed an agreement with a French company to use its software, Linkurious, to visualize connections and follow the money more easily. In these two projects, we created the base of the stack that would later allow us to move quickly on the Panama Papers. As our tools and platforms solidified, the number of journalists working on ICIJ projects and their engagement grew. LuxLeaks (2014) involved more than 80 reporters in 26 countries. Swiss Leaks (2015) more than 140 reporters in 45 countries. On top of helping reporters secure access to the documents, we performed data analysis – the key to strengthening the articles – and created interactive applications that were among the most viewed items on ICIJ’s website.

**BECOMING ESSENTIAL TO ICIJ’S INVESTIGATIONS**

Leaks were not the only type of data we worked on. In Evicted & Abandoned, a project about how the World Bank regularly failed to protect people displaced by development, we estimated 3.4 million people had been affected in a decade and created a unique database of projects using public data. In Fatal Extraction, we combed corporate data and combined it with information from our reporters in the field to reveal deaths, injuries and community conflicts linked to Australian mining companies across Africa. Within a year, we had grown to a team of five, representing about half of the people in ICIJ’s small newsroom. We added Emilia Díaz-Struck as research editor and hired then-intern Cécile Schilis-Gallego as a data journalist. This is the team I was counting on to help me solve the Panama Papers data challenge after the director called me. Firstly, we travelled to Munich to get the data. Rigoberto flew in from Madrid, Spain. We stayed in an Airbnb apartment which we converted into our base camp to copy encrypted hard drives. During the first meeting with our German colleagues, we discovered the complexity of the data, and one of my first comments to my bosses was: we need to hire an extra developer for the team. A few weeks later, Miguel Fiandor joined us from Spain. The data included mostly emails, but it had millions of PDFs and images that needed to be made machine-readable. We used more than 30 servers in the cloud to process them in parallel to make the first batch of data ready for reporters in less than two months. That was the most difficult part, because after the data was searchable, we used the same tools we had created for the previous projects. In late June, ICIJ had its first meeting with a small group of reporters in Washington, D.C. to kick-off the project, although most journalists joined in September after a meeting in Munich. As the months progressed, the leak grew to be 2.6 terabytes and contain 11.5 million files, which meant we had to continue processing data throughout the whole project. The number of reporters involved also skyrocketed – we had almost 400 when the investigation went live in April 2016. They produced more than 4,700 articles. With more reporters, more needs appeared: we had to create a ‘support team’ to help them with problems over our platforms; we created manuals and conducted training in three languages for people on four continents, and we kept improving our tools until publication. For example, we incorporated a popular feature to search for lists of individuals and know, in one go, if there were any hits. We also updated the public database of offshore companies, making it the most-used product in the history of the ICIJ. Today, it is used by reporters, investigators and authorities around the world to chase tax evaders.

**CONCLUSION**

It’s impossible to know how the Panama Papers would have been without the work of ICIJ’s data team but, for sure, we could not have had so many reporters working on it. We would have missed many stories and would have had less impact. Technology and data worked together to turn the Panama Papers into part of history. As we move into the future, three things are clear to me. One is that massive leaks are the new standard, and we’ll see more – and bigger – leaks. Second, global collaboration is the only way to deal with the complex world in which we live. And finally, data journalism is here to stay. If you don’t believe it, let me share just one more fact: almost three years and half into its creation, ICIJ’s data team now has 11 people.
In general terms, data visualization describes any effort to help people understand the significance of data by placing it in a visual context. Patterns, trends and correlations that might go undetected in text-based data can be exposed and recognized more easily with data visualization software. Data visualization should also engage the visual senses of the reviewer in both its presentation and content. Effective data visualization should be informative, efficient, appealing, and in some cases interactive and predictive.

Informative: The most basic function of a report is to inform the consumer of something and a picture can do this in a universal way. Think of a map, perhaps the oldest form of data visualization, or a pie chart, or a bar graph. Everyone is familiar with these visuals and can quickly infer the intended point they represent. Since we are aggregating data and displaying it pictorially it should communicate the message that the aggregated data is telling us and not further compound the problem that large amounts of data can present.

Efficient: Perhaps the biggest benefit of utilizing data visualizations is the efficiency gained through proper execution. A well designed visual will save the data analyst precious time as it can communicate the message of the data concisely and without ambiguity. It should bring the consumer to a clear conclusion quickly without having to analyze pages of data.

Appealing: Much like a masterpiece draws the viewer in and captivates their thoughts as they gaze at the picture, properly designed data visualizations will draw you in and lead you to the intended conclusion in a visually pleasing way. The proper imagery and color palette can bring a boring spreadsheet to life. I’ve seen firsthand colleagues’ eyes glaze over as a spreadsheet is presented to the group. Conversely, you present the same data to the same group with a compelling visualization and they lean forward and become engaged in the analysis of the information presented.

**BIG DATA**

The emergence of a society interested in, and driven by data, has created a premium for quality, engaging data visualization. It has become somewhat of a buzzword in today’s business world, although not on the same level as the “Internet of Things”, “Business Intelligence”, “Cloud Computing”, or even “Gamification”. Its importance and pervasiveness is evident when you consider that it is interwoven into all of those aforementioned topics. Even so, it carries some cache on its own and is a key component of another popular topic, “Big Data”. Using “Big Data” as an example, in business there seems to be an ever increasing desire to capture...
and consume as much data as possible regardless of whether we know what we are going to do with it or why it is valuable. The term is occasionally used in reference to the amount of information, but more importantly in regards to the unstructured nature and disparity of it. That notion crystallizes the need to connect and communicate information in a more efficient manner than a spreadsheet or report ever could. Of course, summaries or KPI’s can capture the essence of this data, but the magic comes when it is connected and dimensionalized over time to communicate trends concisely in a chart or graph. Never mind the fact that copious amounts of information recorded over years can be summarized succinctly in a visually appealing report that people can understand without having to dissect and analyze the underlying data in depth.

DATA VISUALIZATIONS

Even in the consumer space, or our day to day life, we are constantly consuming data visualizations without really noticing. Chances are, the energy bill you received in the mail yesterday has a bar graph in it picturing your energy consumption over the past 12 months or your quarterly investment statement, complete with pie graphs, communicating your investment allocation alongside of those KPI’s! Ask yourself this, where did your eyes go first? Ok, if it was the bill, maybe the due amount, but most likely you were instantly drawn to the graph and gazed at it for a moment to analyze the meaning before reading further. In the case of the investment statement, you may not have gone much further than the percentage increase over the last period and the pie chart depicting your investment allocation.

A well designed visual will save the data analyst precious time as it can communicate the message of the data concisely and without ambiguity. It should bring the consumer to a clear conclusion quickly without having to analyze pages of data.

All of this to say that data visualizations have become an indispensable part of the business world and an ever increasing part of managing our day to day life in our sophisticated digital age! During the workshop “Understanding data through great data visualizations” we will make an introduction to the visualization of data from both theoretical and practical perspectives. We will start with a brief lecture on the history of data visualization and end with an understanding of why we require the use of graphical pictures to explore and find complex quantitative relationships and thus understand why data visualization is so important today. We will continue the presentation with an explanation of what is a graph, or better said, the formal concept of data visualization; and I will also explain the principles that govern and underlie good data visualization.

Finally, we will talk about the state of the art of data visualization using some examples of visualizations that I have found and have caught my attention for their formal and artistic content.
The bank’s chief executive began by explaining that the new digital era has triggered a radical change in people’s lives, which has forced businesses to adapt their products and services to new customer needs. This technological disruption has given rise to a corporate revolution, not only in the banking sector but also globally. The transformation that has taken place has led to the emergence of innovative tech companies that have claimed the privileged place previously held by firms that seemed invulnerable, and that today barely have a market presence. In fact, seven of the ten companies with the highest stock market capitalisation worldwide belong to the technology sector. It is therefore clear that today’s greatest challenge is adaptation to a change of culture. Flexibility has become vital in order to maintain prolonged business success.

It should be highlighted that this transformation has occurred at such a breakneck pace as to substantially reduce the production costs of these new technologies. This means that there are plenty of products or services that have become accessible to practically everyone, something that was unthinkable in the past.

### CHALLENGES

The digital revolution is global, and society and businesses are interconnected. The environment has changed, and all technological evolutions spread rapidly to the market, which absorbs them almost immediately. Customers’ profiles have also undergone a radical shift: they are increasingly demanding, better informed, and are often better protected by regulations. Customers remain at the heart of the business, and the battle to win their loyalty is more complex.

Mr Álvarez went on to discuss what from his perspective are the biggest challenges faced by European Banking.

There can be no doubt that the greatest of these is to overcome the issue of low returns in the sector caused by various factors, such as negative interest rates, low demand, excessive regulation, the need to employ so much capital, along with inherited problems which mean that financial firms are listed on the Stock Market well below their book value. This makes a restructuring of banking an inevitable expectation in the immediate future. Another challenge is to increase customer confidence, which has fallen considerably after the period of crisis. This goes hand-in-hand with a growing increase in user expectations. The demand is for the services typically provided by traditional branches to be delivered more swiftly and with higher quality via digital channels. Customers likewise expect the clearest and most transparent conditions possible, which can be instantly compared with those of the competition, as well as an offering of bespoke, personalised products, to which they can simply and intuitively aspire. Banking needs to invest so as to fulfil these demands and offer a multi-channel strategy, in which each customer will choose how they access the service.

The third challenge would lie in the considerable competition from emerging FinTech companies. There are a great many new competitors...
attacking the business through commissions, and which have been assisted by the fact that they face much less demanding regulations and lower entry costs to break into the sector. This means that financial institutions have been forced to improve their digital capacity to compete with them, using technological data analysis tools to aggregate, organise and monetise the valuable information held about consumers.

**DIGITISATION PROCESS**

Lastly, the acceleration of the digitisation process is vital in order to be able to adapt to the environment. A number of innovations have played a fundamental role over recent years, such as the switch from Mainframes, large computers to process complex data, to the Cloud, the digitisation of Front Office users, the automation of Middle and Back Office processes, the emergence of new technologies such as Blockchain, Big Data, Data Analytics... which have managed to achieve a considerable cost reduction. It is essential that a new culture be successfully developed: “An Agile Organisation”, to compete with these new incomers, to speed up the delivery of products to the market, and to offer customers better services.

Every company needs to adapt the format of its branches to the market in which it operates, designing them to satisfy customers while also increasing their productivity and efficiency.

The aim is to bring about open banking service platforms for consumers and producers, so as to properly serve customers and provide the option of linking up with FinTech firms and new developers, wherever this would be profitable. Continuous improvement lies in learning, managing to be top in the class so as to achieve the ultimate goal, which is simply to win customer loyalty.

As regards the role expected of Internal Auditing within the Santander Group in this digital transformation, Mr Álvarez explained that this has traditionally been a very strong department within the organisation, with great cultural importance and genuine independence. Technology is transforming the way it works, continuously acquiring greater skills to deal with growing risks in terms of Cybersecurity and the considerable demand for information required by Supervisors.

In signing off, Santander’s CEO stated that the best advice he could give to anyone in response to a changing situation is “to listen to people with humility”.

Success means surrounding yourself with the right team of actively engaged people. The business of genuinely listening is followed by the process of decision-making, change, improvement, for which the essential prerequisite is an open mind and an attitude free of prejudice.

*Summary prepared by Fernando García Zapico*
Why Was the Framework Updated? COSO’s previous ERM framework was published in 2004. Much has changed in the world since then, most notably:

- ERM concepts and practices have evolved. Many of the practices that are prevalent today were not in place a decade ago.
- Lessons were learned from various risk events, most notably the global financial crisis in 2008-2009. These lessons provided valuable information about how to manage risks better, which has effectively raised the bar of expectations.
- Business and operating environments have become more complex, technologically driven, and global in scale. Nobody would question how different the business world is today compared with more than a decade ago.
- Stakeholders expect more information about risk, and in many jurisdictions risk disclosures have increased. This drove the need for better information and reporting around ERM.

These and other factors created a compelling case for the COSO Board to initiate an update to its 2004 framework to ensure the ERM Framework was current and sustainable.

WHAT HAS CHANGED?

The first change is a noticeably different title to the framework. Instead of referring to it as an integrated framework, as was the case in 2004, the new title includes the phrase Integrating with Strategy and Performance. This name change recognized how important effective risk management is in strategy and business performance. However, there were other notable changes to the new framework, including the following 10 key changes:

1. New Document Structure
   The new framework reduced the number of components from eight to five, and those components are reflected as integrated parts of the organization’s business model. The five components are:
   - Governance & Culture
   - Strategy & Objective Setting
   - Performance
   - Review & Revision
   - Information, Communication, & Reporting

2. New Principles
   Similar to COSO’s Internal Control Framework, the new ERM Framework introduced 20 principles that are linked to each of the components. The Framework is organized to explain each of these principles in greater detail.

3. New Graphic
   To reflect the integrated nature of ERM, a new graphic was created, replacing the old ERM cube. The graphic, which is shown below, illustrated the flow of a business model, from Mission, Vision, and Core Values, through Strategy Development, Business Objective Formulation, Implementation & Performance and finally achieving Enhanced Value. The
five components are depicted as “ribbons” weaving through the business model, demonstrating the integrated nature of ERM. Some have likened these ribbons to DNA, which is a good metaphor for the importance of ERM being embedded in everything an organization does.

4. **Focuses on Integration**

Integrating ERM with ongoing business practices improves decision-making and leads to enhanced performance.

5. **Emphasizes Value**

Good risk management not only helps protect an organization from bad things that happen (downside of risk) but also helps the organization pursue more risk to make good things happen (upside of risk). This is highlighted in the definition of ERM, which emphasizes that organizations must create, preserve, and realize value.

6. **Links to Strategy**

The link of risk management to the setting of strategy and business objectives is much stronger than in the old framework.

7. **Links to Performance**

Similarly, the emphasis on strategy and business objectives leads to increased emphasis on improved performance, with the end goal of enhanced value and organizational success.

8. **Recognizes the Importance of Culture**

Culture will have a significant effect on the effectiveness of ERM. The ERM Framework recognizes this with a principle focused on culture.

9. **Focuses on Decision-Making**

Ultimately, performance is enhanced and value created when better decisions are made. The theme of improved decision-making can be found throughout the ERM Framework.

10. **Links to Internal Control**

The new ERM Framework does not replace COSO’s Internal Control Framework. However, the two are closely linked, having similar structures and complimentary approaches. Internal control is one type of risk mitigation response, so in some ways the Internal Control Framework could be considered a subset of the ERM Framework.

**HOW DOES THE NEW ERM FRAMEWORK IMPACT INTERNAL AUDITING?**

Not surprisingly, the comprehensive changes to the ERM Framework can impact internal audit functions. The following outlines considerations for annual or periodic audit planning, performance of individual audit projects, and the role in ERM.

**Impact on Audit Planning** – For annual and periodic planning, internal auditors must understand:

- The organization’s business objectives and strategies to ensure the risks being addressed relate to key objectives.
- The risks to those objectives, and how those risks are managed, to audit projects focus on the risk responses chosen by management.
- The organization’s risk culture and risk appetite to ensure audit projects align with both.
- The approach to review and revision to understand how risk management practices may change.

**Impact on Audit Projects** – When following a risk-based audit approach, internal auditors must:

- Understand which business objectives an audit pertains to.
- Align individual audit risk assessments to the organizations risk assessment.
- Design scope and testing based on management’s risk tolerance, not the auditor’s.
- Report deficiencies in the context of impact on objectives so the reader of audit reports understands why they should care about addressing the deficiencies.

**Impact on Internal Audit’s Role in ERM** – While ERM should be owned by management, internal audit can still play an important role in helping to advance ERM. For example, internal auditors can:

- Educate and facilitate understanding of the ERM components and principles; this will help the board and management best execute their oversight and performance roles.
- Advise and provide input to the enterprise risk assessment, leveraging internal audit’s experience around assessing risk.
- Assess effectiveness of information, communication, and reporting to ensure the right risk information is getting to the right individuals at the right time.
- Evaluate the overall effectiveness of ERM to provide the board and management an objective assessment of ERM’s effectiveness.

**SUMMARY**

The new COSO ERM Framework outlines a much more modern and sustainable approach to effectively understanding risks while seeking to create, preserve, and realize value. Internal auditors can leverage many concepts in the Framework to enhance their role in the organization as they strive to achieve the Mission for internal auditing, which is to “enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight.”
Last year a scandal and a media storm seriously shook Sweden when it became known that top secret information within the registries of the country’s transport systems had been outsourced to be handled abroad without sufficient safety precautions. Investigations initiated thereafter could only come to the conclusion that the information had been severely compromised and there was no way to know the full extent of the damage. What had initially been intended to be a sufficient way to handle IT-operations had instead turned into a security threat for the nation.

When the news hit the media, there was outrage and a demand for more information - and to find out who was responsible. The search included a government declaration of mistrust during which government ministers were dismissed, the prime minister’s secretary as well as the entire board of the agency and the CEO. Several investigations followed including a governmental analysis of the agency, of the events that had led to the scandal, and a constitution committee hearing resulting in serious criticism aimed at the government. Thankfully for Internal Audit however, it had been made clear early that Internal Audit within the Transport Agency had done all within its powers to help prevent what later became a scandal. Thanks to solid risk analysis, recommendations and profound documentation, Olofsson found herself being in a safe place throughout the media storm. The media had particularly noticed - after taking part of the Secret Police’s analysis that was made public during the trust crisis - that Internal Audit had tried to warn the CEO and the board, years beforehand, with no response. This made the media very interested in Internal Audit’s role, and Olofsson was in the focus of the media many times during the following year, and involved in several of the investigations that took place.

Finally, Olofsson went on to receive awards, including a prize from Transparency International in Sweden for integrity and professionalism. During her presentation she shared insights on how your daily work routines can prove to be vital later on, and how solid risk analysis, recommendations and documentation can get you through the most trying times during a crisis of trust, staying strong and professional through adverse situations.

Olofsson shared the following Lessons Learned:

- Solid risk analysis and recommendation is the most important shield to the question we must avoid, or at least have an answer to: “Where was internal...
“Are you where you are supposed to be, and could you answer that question if you find yourself in the center of the next scandal?

- When you find yourself in a media storm, the time for preparing has passed. Make preparing a part of your daily routine, and make sure never to skip on documentation. It may be the only thing that separates you from looking like part of the problem to being a proven part of the solution.

- If you are steady in your risk analysis, documentation and communication, do not fear the media. Getting severe problems out in the open might lead to important changes if you stand your ground.

- When the leaders of the organization refuse to listen, it is more important than ever for the GRC professionals to stick together and lean on each other. Leverage the power you have with your colleagues in the second line, it will make you all stronger against internal politics.

- Seek guidance from IIA, mentor, colleagues etc. when navigating rough waters. Consider possible consequences of each step you take - or don`t take - now and later. Through this Olofsson hopes to spread the message of how to stay professional and courageous through adverse situations. “I hope my story has inspired others to stay courageous and strong when it is most needed - because together, and every day, we must act to build trust for our profession,” says Olofsson.
One of the round tables at the European Conference brought together three leading CAEs from the most important banking groups in Europe to discuss various current affairs issues concerning the greatest challenges faced by internal auditors in the financial sector and what is expected from the profession in the future within organisations.

The three featured panellists shared their extensive experience and offered their own points of view on such issues as the management of their human resources, the trend towards automation in the industry, growing cyber-security risks, the oversight of outsourced activities and the major role of regulators in banking sector activities.

"YOU NEED TO CONSTANTLY AND INSTANTLY ADAPT TO WHAT IS HAPPENING", JUAN GIUTARD

Juan Guitard believes that new technologies are forcing organisations to quickly adapt to the digital world, creating new digital objectives and conscientiously overseeing this technological transformation. In response to the new skills needed in today’s world, auditors must be trained in new digital abilities; bringing together people with extensive experience in the various fields of auditing and those who are technologically savvy about Big Data tools. People must understand what they are doing and know how to harness large volumes of data, working their “digital nose” to use new technologies to successfully develop new tools for improving organisational performance and enhancing productivity. Everything done in the past can be improved upon. Even though the consultancy side of internal auditing continues to grow and so too does the connection with external auditors and regulators, the
New technologies are forcing organisations to quickly adapt to the digital world, creating new digital objectives and conscientiously overseeing this technological transformation.

Second-line controls are needed instead, based on tests used to examine security and data quality maintenance through ongoing assessments of general and cyber-security risks. Sally Clark argues that everybody needs to work together on producing the end product and that people should stop “talking with their fingers and talk with their mouths”. Joint efforts can bring about an increase in efficiency, motivation and learning, as well as solve complex situations more effectively.

“TO RETAIN TALENT, WE NEED TO BE ATTRACTIVE AND PRESENT A CLEAR AND SPECIFIC STRATEGY TO CANDIDATES”, HENRIK STEIN

Henrik Stein believes it is essential to implement long-term training programmes for auditors and develop future professional career plans for employees that include staff rotation options for individuals to enter and leave the department to acquire global experience. Presenting an attractive offer in this war to attract talent from the competitive labour market is fundamental to building strong teams and successfully retaining the most talented workers. Automation has led to the development of more efficient and faster procedures, new tools that are closer to where processes take place, which is where the essence of businesses actually resides. Auditors must learn these new automated procedures and use them properly, making sure that digital techniques are being used correctly and monitoring how risks develop within the organisation. One fundamental aspect is the need for regulators to provide precise guidelines on outsourcing, for the expectations that need to be met to be made absolutely clear and for the various outlooks on the range of situations to be presented. A clear method is needed to deal with this increase in regulations, with inspections and requests for demanding action plans from supervisors. To that end, companies are advised to increase the number of staff they have engaged in this task and to maintain ongoing learning exercises in response to the trends of recent years.

All three experts believe that attracting and retaining talent is essential to building human teams comprised of workers with skills in the new digital environment, capable of communicating properly and with strong Big Data analysis skills. New reliable technology tools need to be developed, the effectiveness of which should be tested regularly and the results from which should be documented and analysed with a view to improving the performance of organisations. In order to offer assurance to the Board, auditing should be constantly re-adapted to the current situation, and have a presence on committees and contact with people while always maintaining its independence. Organisations should engage in ongoing assessment of geopolitical risks with a focus on cyber-security. The importance of outsourced activities is constantly growing and they are becoming the core essence of banking businesses. Hence, the existence of specific and clear regulations becomes vital for tackling the transformation that lies on the horizon in the years ahead.

*Summary prepared by Fernando García Zapico
This year European companies have been engaged in a new mandatory exercise: non-financial reporting. From 2018, under Directive 2014/95/EU, large public-interest companies with more than 500 employees have to include non-financial statements in their Annual Reports. This concerned approximately 6,000 large firms and groups across the EU, including: listed companies, banks, insurance companies and other corporations designated by national authorities as public-interest entities.

How did companies approach this exercise? As a new legal requirement to comply with or as an opportunity to revise their long-term strategy and policies including environmental, social and diversity issues? We all know that sustainability implies long-term goals. Companies have to consider the effects of their decisions and actions on the possibility of satisfying the needs of future generations. And they have to report on how they are doing that.

This is not only a legal requirement. Shareholders and other stakeholders are becoming more and more active in asking companies not only to deliver financial performance, but also to show how they positively contribute to society. They are challenging boards on this issue and demanding that the company is governed with long-term sustainability and a stakeholder inclusive perspective in mind. So although directors are nominated by shareholders, their duties in fact go beyond the interests of the shareholders who appointed them. This means that, to a certain extent, fiduciary duties of board of directors are changing throughout Europe towards a stakeholder long-term oriented governance approach.

**SUCCESSION PLANNING**

Many companies, and boards, are working to be ready to face the new challenges on the basis of concrete plans and goals. But there are, however, a few cases where boards are still dealing with ESG issues only when they are facing big competitive or reputational problems. This means they are adopting a short-term view, which is typical of crisis management, rather than a strategic, forward-looking risk management approach.

It seems for instance that succession planning could be further improved. As an example, the latest report on “comply or explain” published in Italy (Assonime 2018) shows that only 16% of Italian listed companies have a formalized succession plan for executives and senior managers, and in the case of mid and small caps this percentage drops to 15% and 6% respectively. Moreover, a survey carried out by Nedcommunity, the Italian association of non-executive directors, in 2018, reveals that strategic discussions mainly take place when the board has to approve the business plan proposed by the executives, which reveals the

---

**INTEGRATED THINKING FOR INTEGRATED GOVERNANCE**

The presentation was focused on best practices in corporate governance and board work aimed at enhancing the strategic function of the board of directors, the effectiveness of oversight on non-financial reporting, long term value creation of business models and related risk management issues.

**PAOLA SCHWIZER**

NON-EXECUTIVE DIRECTOR, BOARD MEMBER AT EUROPEAN CONFEDERATION OF DIRECTORS’ ASSOCIATIONS (ECODA)
“lagging strategic orientation” of some boards. Directors rarely lead the process, for instance, by defining and approving the company vision and the long-term strategic guidelines, taking into consideration all forms of value and thus also ESG issues. Overall, corporate governance is required to further evolve towards a more “integrated” system, where sustainability issues are taken into account in company management and control processes. This should ensure value creation and beneficial results for all stakeholders in the long term (UNEP, 2014).

LEADING ROLE

What would help boards get up to speed and play a leading role in this transformation towards sustainability? Board composition is the first key success factor. Are the same skills and knowledge used in the past suitable to address the new challenges? Isn’t it time to bring creative thinking, innovative thinking into the board, and to hire some new talent, coming from different pools and thus able to “imagine” a completely different way of doing business? An important contribution might come, for instance, from new directors with expertise in crises and turnaround, new and inter-markets, digital and media, IT, and cyber security.

In addition, the board as a whole should develop a new approach to problem-solving, which might be called “integrated thinking”. This refers to the ability to look for and detect connections between different resources and different types of capital (economic and financial, manufacturing, social and relationship, natural, intellectual and human). This approach would help achieve more effective risk management, less siloed thinking and a wider strategic overview. It would also lead to clearer identification of the organization’s key internal and external stakeholders. In order to enhance integrated thinking in board dynamics, the following actions could be carried out:

- Organizing brainstorming sessions and strategic board meetings with no strict agenda;
- Setting up Strategy or Scenarios Committee, where directors can meet external experts on selected issues;
- Enforcing open and frequent communication channels between management and board;
- Analyzing internal and external ESG case studies;
- Defining goals and measuring ESG performances;
- Developing effective processes, beyond compliance: board evaluation, training and induction, succession planning can help identify and cultivate critical resources, skills and talents.

CAN INTERNAL AUDITORS HELP BOARDS DEFINE AND MONITOR LONG-TERM STRATEGIC GOALS AND TAKE SUSTAINABILITY ISSUES INTO ACCOUNT?

The answer to this question is yes. The Nedcommunity Survey (2018) shows that sustainability issues are mostly promoted by risk & audit board committees. Internal auditors provide important information and assurance to these committees. In fact, they work across the organization and its business units and have a helicopter view of the internal and external environment, which facilitates integrated thinking (Jones P., 2016, Internal Audit. An Integrated Approach, Australian Institute of Company Directors). Moreover, internal auditors ensure consistency of metrics across business units. And as they provide assurance of the accuracy of those metrics, they might also help develop new metrics for complex issues. In 2015, the Italian Association of Internal Auditors developed a new measurement model for risk culture, providing 92 indicators linked to banking business, which are, at the same time, compliant with regulatory guidelines. Most banks and financial companies have applied the model and confirmed its validity. But internal auditors themselves need to be more engaged in the business decision-making process and embed integrated thinking within audit practices. They need to start taking into account information and data which is not traditionally evaluated during audit procedures. Issues such as sustainability and corporate governance represent areas of growth and opportunity for auditors willing to leverage and broaden existing skills (Stein Smith S., Auditing in the Era of Integrated Thinking, IFAC, 2017).

So, ultimately, while boards have to improve their strategic-planning skills and enhance their attitude towards sustainability, internal auditors are in the right position to play a pivotal role in the adoption of integrated thinking and drive important changes in corporate governance and board work.

While boards have to improve their strategic-planning skills and enhance their attitude towards sustainability, internal auditors are in the right position to play a pivotal role in the adoption of integrated thinking and drive important changes in corporate governance and board work.
Red teams consist of business, sector and technical experts who are set up to provide an unannounced forensic test over the security threats and controls in place. Their aim, to exploit any security weakness that may exist. Better the ‘good guys’ conduct a comprehensive test to identify the weaknesses and get them fixed, rather than find out publicly once exploited by the ‘bad guys’. The cost of conducting these ‘safe tests’ are insignificant to the sanctions, fines and adverse reputation risks faced by organizations if the crown jewels are stolen, data is leaked or the business ceases trading due to a ransomware attack.

If set up correctly, a Red Team test will be known by only one or two individuals in the organization, who have commissioned the exercise. This provides the closest assessment to reality for the business. Equally the testers will be provided with very little insight, to ensure the war gaming replicates the field of battle provided to the real attackers. It is also important to note that the types of attacks are not solely focused on Cyber Security vulnerabilities – Red Teams can deploy all means available to them. It has been known, as part of the Red Team test, to place individuals into organizations as contractors, to bribe employees to disclose information, to develop relationships on-line through LinkedIn, set up bogus companies to access the inner circle of the business.... The objectives, scope and approach are always agreed with the individual commissioning the exercise. As a result, it is difficult to benchmark the cost and time to complete the test as they are typically bespoke for each organization.

HOW DO RED TEAMS OPERATE

Red Teams typically sit in the shadows of organizations, unknown to management and access whatever resources are required to meet the objectives agreed. To succeed, there are a few fundamentals to understand when setting up the engagement:

● The Objective of the Assessment: It is essential to identify the objectives for the Red Team exercise – Is it to steal the critical dataset, place code onto the website to copy customer payments details or to test whether the manufacturing line can be attacked and taken over. Whatever the objectives, they need to be the ‘doomsday’ scenarios that management lose sleep about. To help identify the objectives, the Red Team will use reconnaissance techniques to get to know the business and, unknowingly to the individuals, engage management to understand what risks or vulnerabilities may exist.

● Agree the Boundaries: The scope should set out what are the acceptable and unacceptable behaviors’ or techniques. Ideally these should be kept to the minimum as they restrict the ability of the Red Team to operate, but equally, there may be certain situations which are considered crossing the line (for example, approaching the CEO’s family, do not actually bring down the live website but confirm it was technically feasible based on the security breach...).

● Penetration Testing alone is no Substitute for Red Teaming: One common failing is that organizations assume annual penetration testing...
Red Teams typically sit in the shadows of organizations, unknown to management and access whatever resources are required to meet the objectives agreed.

It is important all aspects of the IT infrastructure are in scope when conducting a Red Team exercise -- Traditional penetration tests do not always cover all layers and this leaves gaps in the approach. This creates false assurance for Boards and Audit Committees and Red Teams will ensure a comprehensive penetration test is conducted as part of the scope of work.

**BDO’S INFRASTRUCTURE PENETRATION TESTING APPROACH**

**LAYER 1 - External penetration testing (simple hacker)**
Establish whether unauthorized logical access can be gained via the external network interfaces by a ‘naïve’ hacker who has limited and/or no previous knowledge of your network

**LAYER 2 - External penetration testing (normal level access)**
Establish whether unauthorized logical access can be gained, via external network components by a hacker who has the same level of access as your customers and suppliers, to the target production environment and other key systems.

**LAYER 3 - Internal penetration testing (no access)**
Ascertain whether unauthorized access can be gained via internal penetration and audit testing of your systems by exploiting loopholes in your networks services and resources

**LAYER 4 - Firewall and security systems review**

- Analyze the effectiveness of the policies employed by your firewalls and the infrastructure in place for administration
- Review the operating system configuration for a secure implementation
- Review your procedures and processes for monitoring and reporting of incidents on the firewall
- Review network and host security components, for example, Intrusion Detection.

**SUMMARY**

With the growing threat from Cyber Criminals, State Sponsored activity and Hacktivists, there’s a need for organizations to enhance their countermeasures to respond to the challenges that are complex and significant. The recent attacks experienced by organizations such as British Airways are a constant reminder that Security (whether cyber or more traditional threats) is a Board Level agenda that’s difficult to understand and manage.

Alongside training the staff, hardening your IT environment and strengthening your IT related processes, the use of Red Teams is becoming a core pillar of the countermeasures being deployed.

- The military, and more recently the Financial Services Sector, are utilizing the insights from Red Teams to inform the required improvements in the defenses of their organizations.

So what are Red Teams and how do they operate? The remainder of this article will provide an insight as to why Red Teams should become a core competency within the Internal Audit Functions of the Future.
This session focused solely on the broad level as the European Commission’s Internal Audit Service provides only this type of assurance. The first guidance from the Institute of Internal Auditors (IIA) was published in March 2009 as an IPPF - Practice Guide “Formulating and expressing internal audit opinions” in order to assist in expressing an opinion on some or all of an organization’s governance, risk management, and internal control systems. Whilst still relevant and informative, especially the Appendices, most points are now included in the IIA Implementation Guides for Standard 2450 – Overall Opinions.

It should be recalled that issuance of an OO is not mandatory and is at the discretion of the organization. However when an OO is requested, then Standard 2450 “Overall Opinions” applies:

“...When an overall opinion is issued, it must take into account the strategies, objectives, and risks of the organization; and the expectations of senior management, the board, and other stakeholders. The overall opinion must be supported by sufficient, reliable, relevant, and useful information.” Besides the Chief Audit Executive taking into account, and consulting broadly (see Standard 2450 above), the audit plan should be developed to create a robust framework able to provide sufficient and relevant evidence to support the OO. Suitable criteria need to be established including the risk appetite and materiality thresholds to be used.

The IIA Practice Guide “Formulating and expressing internal audit opinions” is very helpful in the development of key corporate principles to provide an agreed-upon framework against which conclusions can be reached and an OO expressed in a manner that can be understood by management and the internal auditors. Moreover, the Interpretation of Standard 2450- sets out the necessary elements to be taken into consideration in expressing an OO (Scope & time period; Scope limitations; Consideration of all related audits including reliance on other assurance providers; Summary of information supporting the OO; Risk or Control framework; OO itself, whether expressed as positive/reasonable assurance or negative/limited assurance).

In addition, reasons for an unfavorable OO must be stated.

WHAT IS THE INTERNAL AUDITOR OF THE EUROPEAN COMMISSION’S OVERALL OPINION?

The Audit Universe of the European Commission’s Internal Audit Service is divided into approximately 385 Non-Financial and 220 Financial processes (about €160 bill. p.a.), thus making it a complex environment but one in which an adequate framework to support the OO has been established. The European Commission produced its first OO for the financial year 2010, having previously prepared one as a ‘dry-run’ for the preceding year of 2009. The latest annual OO was expressed on the financial year
The European Commission’s Internal Audit Service focuses on the state of the European Commission’s financial management and is based notably on work conducted over a period of 3 years by the European Commission’s Internal Audit Service and takes into account the reports by the European Court of Auditors which is the EU’s Supreme Audit Institution or external auditor. It also relies on the assurance provided by other internal functions, notably from the 1st and 2nd lines of defense (Line management, risk managers and internal control specialists) and the OO is subject to management reservations already expressed under the financial and risk management framework.

WHAT IS THE ADDED VALUE OF AN OVERALL OPINION?

The OO provides assurance to Stakeholders attempting to assess the overall state of play of the financial management system of the organization. It gives added-value to the many internal audits performed as these are used as the basis for a global assessment underpinning the OO. Besides the efficiency and effectiveness of this action it also motivates audit staff to see how their work fits into a bigger picture.

HOW DOES THE OVERALL OPINION HELP THE EUROPEAN COMMISSION?

In general the experience of the European Commission’s Internal Audit Service, with 7 continuous OOs under its belt, has been positive and plays an important role in the Assurance and Accountability chain. Moreover it has also contributed to raising the profile of the service across the organization, of staying more relevant to the business and earning a seat at the top table!

The Overall Opinion provides assurance to Stakeholders attempting to assess the overall state of play of the financial management system of the organization.

WHAT BURDEN IS IMPOSED?

The burden is directly on the audit staff but should not be exaggerated as once it is embedded into the risk assessment and audit planning environment the overall workload is manageable, especially considering the positive reception given to the OO. It has negligible impact on the audited services.

WHAT’S THE DIFFERENCE BETWEEN THE OVERALL OPINION AND ALL THE OTHER REPORTS PRODUCED EVERY YEAR?

The OO is not a panacea, something that will radically change the perception of the state of play of the corporate financial management system. It is based on a well-founded framework that needs to be reviewed on a regular basis to ensure that it stays up-to-date with the evolving organization-wide systems of control. It has a place within the financial reporting-architecture of the European Commission and is even referred to as a key assurance point in an annual report to the European Parliament and the Council.

WHAT COMPARISONS CAN BE MADE WITH THE AUDIT OPINION OF AN EXTERNAL AUDITOR AND, NOTABLY, IN THE PUBLIC SECTOR, THAT OF A SUPREME AUDIT INSTITUTION (SAI)?

In the specific case of the European Commission, which has a large budget [about €160 billion p.a.] that is audited by the EU’s Supreme Audit Institution, it is instructive to compare the annual Statement of Assurance on the legality and regularity of transactions underlying the annual accounts issued by the latter with that of the OO issued by the European Commission’s Internal Audit Service.

The focus of the EU’s Supreme Audit Institution audit opinion is on the audit trail from the European Commission to the level of the final beneficiaries whereas the European Commission’s Internal Audit Service concentrates its examination on the European Commission’s internal control system. The perspective of the European Commission’s Internal Audit Service is annual, focusing principally on error rates obtained through substantive testing of statistical samples whereas that of the European Commission’s Internal Audit Service is a multi-annual one based on a comprehensive reference framework and professional judgement.

Moreover, the purpose differs also in that the European Commission’s Internal Audit Service provides reasonable assurance to external stakeholders and is the basis for the discharge by the European Parliament (after consultation of the Council) on the implementation of the European Union budget. On the other hand, the European Commission’s Internal Audit Service provides reassurance to its governing body, the College of Commissioners, on whether governance, risk management and internal control procedures are adequate to give reasonable assurance over the achievement of its financial objectives.
Since our job basically consists of gathering and analyzing information, and since the businesses we audit are transforming to incorporate more data-based automatons in their processes, mastering data analytics clearly appears to be the future of audit. Pursuing this ambition first required activating all possible levers at hand to massively change the way our audit teams carry their analysis, and lead them into exploiting the potential of larger data sets, using data visualization and basic data analytics techniques. Then, since we evolve in a complex data environment – large volume of data, structured or not –, and since we believe that some complex technologies – such as neural networks – are extremely relevant solutions for many of the problems we deal with in our analysis, we have built a fully operative team of data scientists and IT experts to accompany this change. Concretely, the challenge is to build a new job from scratch - data scientist for audit - and meticulously finetune the interaction between these new experts and existing audit functions, in order to capture as much value as possible. Consequently, this new era of auditing requires managing complex technicalities, such as developing a deep understanding of new regulations on data protection and equipping ourselves with more powerful tools and infrastructures. Henceforth, we have set the grounds to develop further a strong technical expertise and create a known data science franchise, by participating in the academic research community. Moreover, thanks to a facilitated access to data and to our ability to tackle the bank’s problematic, unbiased by existing solutions or processes – we are not reviewing processes, but trying to beat them –, audit is a perfect place to explore new approaches based on data analytics: the next challenge is to transform punctual high added value case studies into industrial solutions, which we can value, and mutualize with others within the Group. We have reached the critical size and maturity to establish win-win partnerships with other data teams from the firm, with the ambition to participate actively in the definition of the Group’s data strategy and be a strong driver for its development. Besides being a fantastic, and unavoidable, lever to attract and develop our teams, this strategy and corresponding investments have already increased our efficiency, robustness and challenge capacities, and enabled us to bring more added value and be credible game changers for our firm. Thanks to data science and technology overall, we are establishing a new business model, at the crossroads between an audit team, a R&D department and a startup.
Todo lo que necesitas saber sobre Auditoría Interna, Control Interno y Gestión de Riesgos a un click

descubre nuestra TiendaOnline en
publicaciones.auditoresinternos.es
Within the Oil & Gas industry, partnerships are used as vehicles to minimize risks and boost performance: by reducing the working interest in each operation, partners maximize exploration success. Other less tangible benefits from being in an association include sharing of technical prowess, financial strength across the partnership and local knowledge. Also, host Governments can look favorably on a mix of domestic and international experience when developing its natural resources.

Each party in a Joint Operation should ensure the right internal control environment of the part of the processes is responsible for, but agreements reached between the parties may also provide for audit rights to verify the compliance of the parties with the contractual provisions. Audit rights available will depend on the nature of the agreement, and vary from internal control to contract compliance type of audit work. The type of partnership also determines the degree of involvement of each partner in joint operations and its associated legal responsibility: from the fully owned and operated asset to the non-operated joint venture model, the Oil and Gas industry has a broad spectrum of types of partnership available for managing its assets:

As activities become more complex and globalized, the involvement of partners in the performance of operations provides challenges and opportunities for most Organizations and their respective Internal Audit functions.
In this summary we will look at two basic types of association agreements between partners to establish Joint Operations: Joint Companies (Shareholders agreements) and Joint Ventures (Joint Operating Agreements). Each of these models has their own unique characteristics, benefits and opportunities.

Joint Companies are essentially standalone businesses where a number of partners will have a shareholding interest. The shareholder agreement is the master document that regulates the partner obligations, the frame in which the partnership will operate and it will define audit rights available. When negotiating the shareholder agreement, it can be advantageous for Internal Audit if the audit rights are broad providing greater access to the business. Joint companies typically have their own Board of Directors populated by representatives from the parent companies, its own employees (although it is common that partners temporary assign secondees to the joint operation) and will enter into its own contracts with vendors, suppliers and contractors. As these are standalone companies, they usually generate their own financial statements.

**AUDITS IN THE JOINT COMPANIES**

When planning audits in the Joint companies it is important to remember that these companies will have their own standards and procedures may be independent, inherited from one of the parent companies, or even a hybrid. Auditing to different standards than your own can be a challenge for the audit team; however this can also be seen as a good development opportunity and motivator as they are working in a different environment. It is important to recognize the strengths in each of the partners’ audit groups and utilize these skills properly. It is essential that the parent audit groups are aligned throughout the entire audit engagement. The audit team should provide the Joint Company with a single audit plan and an aligned set of recommendations. Joint audit work will provide a common understanding of the control environment to each of the partners providing the opportunity for aligned messaging and initiatives to improve the Joint Companies control environment. It is important to note that there may be no contractual requirement for the Joint Company to adopt the recommendations of the audit. Influence will be key in these cases, having secondees in the business can facilitate getting the recommendations implemented.

In the case of Joint Ventures, a private agreement called Joint Operating Agreement (“JOA”) regulates the relation between the partners. The Joint Venture is an entity with no legal personality: one of the partners acts as “Operator” and is responsible for day to day activities, while the “Non-Operators” cover a portion of the expenditures (the Operator submits the partners with lists of costs incurred during the preceding month) and are entitled to its share of production. Employees belong to the Operator, who is also responsible for entering into contracts with the contractors/vendors. Operations are subject to budget limitations, approval of expenditures, Operating Committee discussions, etc. Each partner is responsible for generating their own financial statements.

Joint Operating Agreements usually limit audit rights available for the Non-Operators to the verification of the expenditures and revenue associated with the Joint Operations. The Non-Operators usually have deadlines to raise claims and if audit rights are not exercised within the contractual period, the amounts rendered by the Operator will be considered as definitive and not subject to further adjustments. While reviewing expenditures and revenue for contract compliance, monetary adjustments can be identified, which can represent an efficiency tool for organizations.

The Operator performs activities following its own norms and policies, which are not usually subject to audit by the Non-Operators. The limited audit rights available in the JV require a risk assessment of the Operator before entering into the JOA, in order to guarantee that internal control of the JV is aligned with Non-Operator’s internal control expectations.

**SUMMARY**

The world is changing towards more collaborative environments and audit functions have to adapt and help the business achieve its goals. In Joint Companies, collaboration is essential between parent audit departments, to minimize disruption, add value and ensure adequate control in the business. In Joint Ventures the Operator should assure an adequate internal control environment in Joint Operations, while audit rights available can be used as a cost efficiency tool for Non-Operators.
Apart from deep technical aspects, let us say that a blockchain network is a set of connected computers that shares a file among them. Anyone in the network can append a post to the shared file and immediately any other computer in the blockchain network will be able to see it. The post is signed digitally, so everyone could verify the authenticity and the integrity of the post. To be sure that no one could trick the data, each post includes the signature of the previous post in the file, so when the new post is signed, the safety of each previous posts is also hardened. These chained signatures are remarkable because they prevent that any Information could be deleted. It is also worth mentioning that no central servers are required.

The core characteristics behind blockchain are verifiability, transparency, disintermediation, value transfer, immediacy, automation and competency. The information written in the blockchain is digitally signed, and digitally timestamped with state of the art public key cryptographic protocols, the same used in legal digital signatures stated in European EIDAS regulation. This makes it possible to know who posted the data, when it happened and verify that it has not been modified.

**VISIBILITY LEVEL**

A blockchain network can have the visibility level that we may need. From very public information, to permissioned access for only a few people, or private to a closed group of users. By setting the visibility in the correct way, the information can be transparently shared to the stakeholders in a safe and reliable way.

We stated above that no central servers are required, so a consensus protocol is needed in order to achieve a global agreement on the correct order of the posts in the blockchain file. This could be provided by several algorithms that can be used, and depends on the degree of confidence between participants. For the records, some of the approaches to achieve a consensus are proof of work, proof of stake, proof of authority and proof of elapsed time. But explaining them is beyond the scope of this paper, so simply consider that a decentralized consensus is achieved.

Regarding value transfer, it is worth mentioning that the very first use for which blockchain was intended was for digital money. With that in mind, it is common to find the terms “ledger” for the so-called blockchain shared file, and “transactions” for the mentioned posts. And each transaction was originally an annotation stating that the user A transfers X crypto-coins to user B. Despite a consensus algorithm, that could take a few minutes to propagate a transaction worldwide in the worst case, it is almost immediate compared with the time that takes a cross border swift money transfer. It is a question of minutes compared to days: practically immediate. In the last generations of blockchains the concept of “smart contract” or “chain code” was introduced. It is no more than a program that runs in the blockchain nodes, and can communicate with other users, other contracts and are able to transfer money under programmed
The very first use for which blockchain was intended was for digital money. With that in mind, it is common to find the terms “ledger” for the so-called blockchain shared file, and “transactions” for the mentioned posts.

management, certain information can be posted to the blockchain: the conditions of the request for proposals, the publication and invitation, the proposals provided, the formulae to evaluate the proposals, etc. A smart contract will apply the formulae, will rank the proposals, will register the winner and log the contract and its characteristics. For the sake of internal audit, we have identified these controls: 

- C01: No. of bids below the minimum required
- C02: Submission of proposals after the deadline
- C03: Penalized clients that are restricted from submitting bids
- C04: Lack of additional documentation necessary for bid submissions
- C05: Documentation not uploaded correctly to the tool
- C06: Format for bid submissions not accepted
- C07: Incorrect award at lower price
- C08: Non-compliance with occupational risk prevention rules
- C09: Incorrectness of professionals’ documentation
- C10: Technical and qualitative capabilities of the professionals in accordance with the provisions of the technical proposal
- C11: Adaptation of the specific clauses to the updated legislation (GDPR, third-party liability, etc.)
- C12: Submission of economic solvency documentation and verification of its accuracy
- C13: Review of being current in obligatory tax payments at the appropriate rates
- C14: Verification of authorized personnel by working area
- C15: Correct allocation of the cost of hours according to the work performed (maintenance/repair)
- C16: Verification of the chargeability of overtime hours at the correct time
- C17: Parameterization of the maintenance and repair tasks in accordance with the established hours/task ratio

However, blockchain is not only useful to log functional information. In the field of Internal Audit, these blockchain characteristics can be combined to build systems that implement automated audit controls, that log the result of these controls in a reliable way, that raises alerts where controls failed, and that ensures that these alerts are attended and tracked until they are closed. Every step is logged in the blockchain, as well as the evidences that support them. Every log entry is timestamped, so there will be no doubt about the moment when it happened. Each event will be digitally signed, so the users will not be able to repudiate the facts. And smart contracts will ensure that relevant stakeholders are informed.

As stated above, for the time that blockchain as a technology has been with us, the convenience of its characteristics and the ability to apply them to concrete use cases that improves the practice of internal audit, it makes sense to conclude that blockchain and internal audit will be tightly tied into the near future, and for a long time to come.
With a brilliant presentation, Hervé Gloaven shows us the principles that underpin integrated auditing at Allianz. The Allianz group is an international insurance group with a team of more than 545 auditors. These auditors produce more than 1,000 audit reports that must be consolidated at a group level and convey the most significant aspects to the Audit Committee of the Allianz group while providing value and recommendations for improving the governance, risk management and internal control systems in line with the group-wide corporate strategy. Hervé Gloaven believes that the key lies in finding a balance between enough decentralisation to remain informed and meet obligations with local stakeholders and the provision of value within a consolidated international group structure. No less important is the need to have a strong standardisation process that allows for auditing under strict methodological discipline capable of focusing on the strategy – the previously defined major risks – and providing consistency, comparability and aggregation in the work undertaken at both a local level and throughout the group structure.

**KEY AREAS**

Three key areas are highlighted in the presentation by Allianz:

1. **Decentralisation**
   This mainly enables local assurance with the regulators of the countries in which the entity is located to be guaranteed and specific requirements to be covered in the local perspective, especially regulator expectations. The requirements imposed in Argentina are entirely different to those imposed in Arab nations. The main focus for internal auditing is local assurance. Auditing teams should oversee the design and operation of internal control systems at the various local entities and guarantee assurance and recommendations for improvement. The essence and specific characteristic of each country should not be lost. This is what Hervé Gloaven calls “the coffee machine effect”. It provides specific knowledge about what is happening in each market and each entity. You should be up to speed with “what you hear around the coffee machine”. In other words, you should know what is actually happening at the entities; what the culture is.

2. **Integration and consolidation**
   The difficulty lies in balancing local interest with group-level perspective and expectations. The key lies in ensuring that the content of interest in local audits, in each country, forms part of the entity’s global strategy, and that local interests and obligations are relevant from a group perspective. Audit teams need to take part in audit planning by the group, and need to be able to provide input to convey the emerging risks that arise at a local level and their aggregate impact for...
It is essential for local teams to know what the group wants to audit, what the internal corporate audit strategy is, and why and for what purpose a risk is audited according to the business strategy. Ongoing communication must also take place with the various stakeholders, not only with the community of internal auditors but also with such others as management and leadership, the regulator, audit committees and boards of directors, shareholders and other key positions (actuarial, risks, compliance), etc. It is necessary to know and align the expectations of each one regarding the role of auditing. Communication between the group and local auditing teams is a fundamental piece of the puzzle. Hervé Gloaven tells us about the communication and ongoing collaboration model in place at Allianz between the group auditing team and the local auditing directors and/or managers during the planning stage, development of work and conclusions from the results. To enable this integration, guarantees must be made that the work undertaken by the various teams at the different local entities is consistent and comparable. A standardisation process is therefore essential beforehand.

3. Standardisation
A common pattern needs to be created so that the integration process can be based on common ground and auditing can be undertaken according to certain rules wherever it may be. A common methodology within a set of specific parameters. Hervé Gloaven says this standardisation should take place around certain clear cornerstones, which he calls “APP” and which constitute the basis for the auditing model developed by Allianz. It involves:
1. ASSURANCE
2. Auditing PRACTICES
3. PEOPLE (the people and resources undertaking the internal auditing activity)
4. TECHNOLOGY (technology environment in which the auditing model must be developed)

**ASSURANCE**

The concerns or demands identified at a local level must be conveyed upwards (what Hervé Gloaven calls “not missing the elephant in the woods”: emerging risks) and local teams must know about the clear strategy and scope for the group in terms of auditing. Sound knowledge of expectations from the group and its stakeholders at both group and local levels allows for integration based on decentralisation.

**PRACTICES**

It is important to define closer ties to the assurance tasks undertaken for the organisation as a whole. One example of this would be to structure the internal auditing work into large blocks that can enable a methodology and closer ties to the common risks throughout the organisation and in all local auditing units. As can be seen in the image, the Allianz model is structured into eight main assurance blocks adapted to the group operational model and the nature of the risks and business undertaken: Life&Health; Investments; Operations; Legal and Compliance; IT; Finance; P&C and Reinsurance; Marketing.

An auditing perimeter or universe has also been defined through 73 standard auditing activities or targets (Master Audit Universe), as well as a catalogue of audit programmes for each one. This means that all auditing activity follows similar parameters at an operational level regardless of the geographical area in which it is undertaken: estimated work duration times for each target, standardised reports, work programmes, etc. These standardised patterns facilitate comparison and increase consistency between work done at a local level, as well as aggregation at a group level. Allianz issues some 1,000 audit reports a year. Although this way in which local teams approach auditing might sound simple, it has led to many problems because it has even required the development of a single language for use throughout the organisation: identification of processes, common nomenclature, etc. It has also allowed the risk assessment process to be standardised, thereby enabling the comparison and assignment of levels of diligence when overseeing said risks: similar audit activity times for similar impacts on the risks, etc. This facilitates comparison between projects, and their integration and consolidation at a group level. A series of minimum and maximum work time parameters exist for each auditing activity in order to set aggregation frameworks for
Auditing teams should oversee the design and operation of internal control systems at the various local entities and guarantee assurance and recommendations for improvement.

motivated and able to learn from the entire local and group structure. Tasks need to be rotated within teams and even in the audits that are undertaken throughout the organisation. The audit function should provide general and specialised training in the skills needed to do a quality job. It should allow teams to acquire new skills from analytical solutions, from specialised experts in certain risks, guaranteeing global coverage of the risks and a broad range of skills.

TECHNOLOGY

New technologies and the exhaustive analysis of risks by local and group level audit teams are allowing audit oversight work times at the Allianz group to be highly varied, thereby shortening finance and operations audits while extending audits in the fields of technologies and emerging risks, such as cyber-security.

In short, Allianz summarises the 10 keys that allow it to achieve balance between audit expectations at a group level and assurance within local audit teams. These keys can be seen in the image below, guaranteeing broad coverage of assurance at a local level while respecting the local perspective and demands in the various countries where the group operates.

*Summary prepared by Sonia Vicente Alonso
This presentation offered to attendees several ways on how to maximize value of a lean internal audit function in a large multinational company. The presentation is based on practical experience and examples from internal auditing within CEZ Group. CEZ Group is an established, integrated electricity conglomerate with operations in a number of countries in Western, Central and Southeastern Europe, headquartered in the Czech Republic. Its principal businesses encompass generation, trading, and distribution of power and heat, as well as coal mining. Apart from the production and sale of electricity, CEZ Group also deals in energy services, venture capital, telecommunications and nuclear research.

CEZ Group has undergone a significant transformation in recent years where the internal audit played its indispensable role as an internal control guard and strategic advisor. We, the CEZ Group internal audit, had to transform ourselves to be able to play that role. The way we do internal audit now is called “Smart audit”.

Smart audit combines several auditing approaches from conscious motivation of auditors, through ongoing negotiation of stakeholders needs and the related role of IA to well considered auditing methodology:

- **Self-reflection** – what do I want from my life, my profession, my job?
- **Knowing your stakeholders** – Who they are? What are their expectations?
- **Positioning of the internal audit function** – what is the most beneficial role of IA right now?
- **Well considered auditing** – how to perform audit engagements with minimum effort and maximum impact?

During the presentation practical tips from internal audit planning, managing and marketing will also be shared.
Disruptive forces are causing organizations to consider transformation plays. Businesses must deal with challenges caused by the digital revolution: the move to digital processes and business models; complex regulatory oversight; proliferation of social media and disruptive new technologies that promote increased connectivity and a demand for new skills. Internal Audit has to evaluate if the function is ready to digitalize itself, to lead the “digital journey” for the organization and to take on the challenge to deliver more comprehensive solutions? This article offers highlights on how internal audit functions need to act and respond to the digital revolution. It is designed to be provocative. Our Goal is to stimulate new thinking and challenge current paradigms. Each organization’s journey will be different and unique. Internal Audit has been “transforming” for the past 20 years, making incremental improvements that have helped the function do the same things faster (limited data analytics and selectively leveraging technology) with a better focus on risks (risk-based audit plans); however, the basic approach and methodology of Internal Audit have not substantially changed — most functions still audit in much the same way they did in the 1990’s. This traditional paradigm may impair Internal Audit’s ability to transform rapidly, leaving a risk gap. Internal Audit needs to alter the way it operates to become better in what is done today and to become more relevant. Internal Audit’s core mandate will be delivered with significantly reduced effort and headcount. At the same time a shift to become a Change Agent, Anticipative Monitor and Business Counselor. IA functions will incorporate multiple facets of the following mandates:

1. The vision of a fully digitalized internal audit function including the technological approach, prerequisites for the governance as well as for the people model, needs to be streamlined to stakeholder needs. The mandate of Internal Audit will evolve from the baseline Assurance Provider to become a Change Agent, Anticipative Monitor and Business Counselor. IA functions will incorporate multiple facets of the following mandates:

a. Assurance Factory: Focus on non-negotiable assurance and base level of trust and current / past topics with findings with respect to the current impact of recommendations to raise awareness on current / past topics

b. Change Agent: Focus on trends on why things fail systematically and audit against “unknown” rules.
Findings reported based on deep dive in root-cause analysis based on internal best practices for recommendations to initiate change within the organization

**c. Anticipative Monitor:** Focus on future topics (e.g. missing controls, policies & procedures) with findings reported with respect to future impact of recommendations to anticipate how the business model is changing

**d. Business Counselor:** Focus on strategic topics and actively engaged in strategic discussions and problem solving. Findings reported with respect to anticipating the future / industry trends and the impact on the business to foster change and best practice development and sharing.

2. The methodological approach to create the function including the transition roadmap needs to be strongly based on innovation and latest (available) technology. Internal Audit functions will need to consider at a minimum the following elements:

**a. Digital Excellence:** Efficient analytics delivery and optimized operations through further process standardization

**b. Off- / near shore hubs and flexible workforce to be leveraged**

**c. Disruptive Innovations:** Predictive and prescriptive Analytics, Audit of emerging risks and robotics / Internal Audit enabled audit procedures

**d. Enhanced internal collaboration across the 1st and 2nd line of defense**

3. The practical application of significant parts of the concept across the digital value chain needs to be implemented on a step-by-step basis (during our presentation showcased at the example of the internal audit function of Sandvik AS), such as:

**a. Starting with descriptive analytics to set the baseline for prescriptive and predictive analytics**

**b. Re-shuffling work to be done between the human and the machine by giving [Artificial Intelligence-enabled] robots more and more tasks to perform audit procedures and enhance back-end processing**

**c. Re-inventing the risk assessment process by continuously assessing risks and center everything around risk analytics in the core**

**d. Implementing new ways of communication based on interactive dashboards and video reports**

**e. Using natural language processing technology to establish an interactive audit assistant (such as Siri and Alexa)**

In our vision, Internal Audit can be viewed like an air traffic control tower. We believe that the current technology will enable continuous auditing and timely reporting of high risk findings. This operating model will also enable a higher degree of flexible sourcing and will feature an agile and dynamic process, enabled by technology that allows the function to respond to the evolving risk landscape.

**SUMMARY**

Internal Audit must incorporate emerging technologies (robotic process automation, artificial intelligence, machine learning, etc.) as part of this new operating model. This will also allow a variety of dynamic outputs to be utilized on a more real-time basis to deliver feedback based on the needs of different stakeholders. A new workforce model, enabling Internal Audit to focus on purposeful, value-added work will also be required. These changing workforce dynamics will require Internal Audit to develop a more flexible, adaptive and collaborative work environment. While we originally thought that vision would be realized in about 2 to 4 years, we are thinking it may be shorter, considering the pace of digitalization we are experiencing at EY and seeing at some clients. The journey has already started – where are you today?
As evidenced by recent media coverage, cybersecurity has quickly become a central threat to modern organizations. Spanning espionage, ransom, insider threats and foreign government infiltration, the cybersecurity challenges of today are enormous -- both in scale and in complexity. Sadly, the systems we use to defend against cyber attacks are also alarmingly ineffective: 97% of companies remain vulnerable, only 53% of attacks are even detected by internal cybersecurity systems, and each attack that was spotted took on average 99 days to be detected.

From a risk perspective, these attacks add up fast. Across the financial, ICT, transportation, critical infrastructure and services (healthcare, government and energy) sectors, the loss from cyberattacks ranges from €1.6 - 10.8 million/year per organization or €208 billion/year (1.6% of GDP) in the European Union alone. Simultaneously, the number of cybersecurity incidents worldwide has compounded from 3.4 million in 2009 to more than 59 million in 2015. A cynical takeaway is that if you could invest in anything, you should invest in cybercrime! But a natural question is instead: what could we possibly do?

**MY ANSWER: YOU SHOULD THINK LIKE A HACKER.**

I claim this because I grew up as one. I have been on the other side and experienced the power and capabilities that makes the hacker underground so alluring, and yet so dangerous. Being in the underground gives a unique perspective on understanding both how and why our defenses are so weak. (I recount some of these aspects in my talk.) Crucially, the experience gave me a mindset, which I call the hacker mindset: the instinctive and repeated question “how can I break this?” I argue that by having people in your organization regularly ask how they could break in, you will be able to mount better defenses.

Let me explain. First, let’s agree that the definition of “security” is opaque. The word quite literally means the absence of vulnerability. But how would you expect to “get” or “measure” security without understanding what those vulnerabilities might be? Without ability to understand how you would find or exploit flaws in a system, what hope do you have to stop others from doing the same? You first need to imagine that someone might try break into your building through an open window to have the foresight to lock the windows. Defense and attack are also inherently asymmetric activities. The hacker needs only to find one way in. But you, as a defender, must anticipate every possible way someone might try to take to break in. Supposing the people in your organization were simply unaware of certain new kinds of attacks, then those become the weakest link that hackers can use to break in. You might even remain fully unaware that these attacks even took place! With the rise of cybercrime, the rate at which such novel attack vectors are discovered is unfortunately rising.

As a Professor, I have been teaching cybersecurity for 7 years. Ultimately, your role as an internal auditor is to help minimize risk to your business or organization. But what are some of the critical risks that are overlooked?
When I see that the most common vulnerability kinds remain the same today as they were 10 years ago, I feel that we have failed as educators. Too many of our graduates are unaware of this critical hacker mindset and thus continue to produce insecure code that now increasingly come back to haunt us.

As an internal auditor, I plead to you that you should help your organization adopt processes that train and continuously apply the hacker mindset. The impact can be enormous. For your developers, for instance, investing in raising awareness of software vulnerability types by allowing them to understand how hackers would misuse them means that they are better equipped to avoid making such errors in their own software. The approach is cost-effective: fixing a defect after the software is already deployed in production can cost 95× more than addressing the issue in previous stages, which may involve system downtime, damaging the brand, loss of customer trust and even liability costs.

If thus adopting the hacker mindset reduces incidents even by only 10%, each company reduces damages by €160,000 to €1 million per year on average, saving EU organizations more than €20 billion annually. It is, however, notoriously hard to find qualified instructors for security training.

Along with colleagues, I decided that is a problem to be tackled at scale. In addition to giving talks, we created an online web platform (adversary.io) for cybersecurity training that helps you understand how hackers would misuse vulnerabilities – helps you adopt this hacker mindset. The platform allows the people in your organization to put themselves in the shoes of the attacker and learn why vulnerabilities arise, and thus they begin to understand how to properly mitigate such mistakes. The training is entirely hands-on, instead of the knowledge-based focus we have used in academia. We used gamification to make the platform fun and engaging for employees to learn about security problems and this mindset. Also, when new attacks and types of vulnerabilities come out, we update the platform contents so that the users stay abreast of the cybercriminals and better manage their risks.

For managers, we built the platform to allow them to monitor individual employee progress, giving a rare measure the security understanding of one’s employees, identify technical areas of improvement for the teams, and even help evaluate security know-how during the recruitment process. Based on their needs, managers can define specific training campaigns for their teams, such as to meet required certifications like ISO/27001 and PCI.

CONCLUSION

You, a Super Internal Auditor, can tackle cybersecurity concerns head-on by ensuring your company actively trains personnel to understand not just the mitigations, but the security problems themselves: you want all of them to realize that the window is an easy way in and should be locked. An active hacker mindset can truly decrease the risks to your organization.
These challenges are greater than ever due to the fast changes businesses are facing globally. To better understand these challenges, this discussion panel counts with highly skilled Board Members / Chairs of Audit Committees of some of the finest and most distinguished companies from Europe.

Audit committees from different businesses agree with the fact that they face several threats from political and economic uncertainty, as well as regulatory compliance (especially aligning local and general laws and regulations). Let’s not forget the “not so new” digital revolution the world is facing which impacts businesses on a global scale and is a disruption threat that concerns audit committees.

How can audit committees get a clear idea of the business and its associated risk exposures?

Gilberte Lombard. When I was appointed board member of the Audit Committee I asked them to teach me how the company and the sector worked, because I am not a specialist. I also asked to read the minutes of the Committee meetings for the last three years to see what the most important audits and risks were. I spoke with the Internal Audit Manager and about his relations with the Committee. I also asked to learn about the different departments of the business and the account auditors. That is how I learned.

Clare Thompson: I’d add two things: we can be on more than one audit committee; and what you learn on the board of directors of a company you can use when you are board member on another. Another advantage is having external contacts and events such as this in which you can learn.
Melvyn Neate: To try to know the business it is important to know which what the committees on which important decisions for the organisation are taken are, so that they invite you. I tend to go to the internal audit department and ask them to bring me up to date with the organisation, and they tell me things that I couldn’t find out otherwise.

Significant aspects of ignoring risk. What do we expect from internal audit for risk assurance?

GL: In internal audits ignoring the risk has to do with the risk management team, if it is separate, because they work closely together. We have the opportunity to carry out a joint test between internal audit, risk management and internal audit, to measure all the risk controls and supervisions. In our case we present the risk map before and after the mitigation, which allows us to highlight the progress or problems that have arisen over the year. The audit committee sometimes asks for a review of a very specific risk so that over a year we can cover other more important risks that the company has to assume.

CT: As I come from financial services, I am used to having the risk management and internal audit functions separate. Internal audit must have all the knowledge necessary to cover everything. In all the committees I have been on we have had two accounting firms available and made use the resources of this team if necessary. There are times you need a super expert on a specific subject. Nothing is too difficult for internal audit to deal with.

MN: I expect the internal audit to be sincere, honest. In a large organisation there are many resources, but in a small one there aren’t, and internal audit must provide me with a sufficient level of assurance or tell me if I don’t have the necessary resources, in which case I could help them. Co-sourcing works well in many cases, and they should also do it in small organisations.

According to a number of studies, the members of boards of directors tend to be satisfied with the quality and frequency of internal audits and their communication. What steps must be taken by internal audit to reach the level of being considered a trustworthy advisor?

GL: For me they are already trustworthy advisors. I have a direct line to internal audit; they are independent, and I usually try to meet with the internal audit manager to talk in depth and freely about many issues. They have also invited me to the annual seminars of the internal audit team, something we were very grateful for, because we realised that the audit committee is more than just a committee that appears on paper. It improves trust because the internal auditor can talk to me about specific risks that have been discovered, describe the risk and how to mitigate it.

CT: To consider them as trustworthy advisors, the internal auditors must know what the directors need. For me, what is useful is that internal audit talks about the business and the root causes of problems. Not only the discoveries; they should go beyond that and give opinions on the business, not only on processes. This makes them trustworthy advisers.

MN: We must ask internal auditors what is of concern to them, have a sincere and confidential conversation with them, inspired by trust; Know whether they act in silos or coordinated with internal control, risk management, compliance...

But above all, the audit committee must see how internal audit is considered by the business. If they are seen as value aggregators, etc. More emphasis has to be placed on internal audit offering a more general vision, because it can interpret all the separate pieces of this great puzzle that is an organisation, and provide us with an overarching view.
Are audit committees sufficiently focused on reputational risks and controls related to them?

CT: When there is a problem of reputation and a problem of trust in the organisation, that is really serious problem. This must be a priority on the agenda. In my world there are many experiments with stress tests, and there we see hypotheses that must be considered about what could happen and how to act in that case. Many reputational risks lie beyond control (third parties, government actions, etc.) and are very difficult to control.

MN: Almost any risk involves a reputational risk, and one that in many cases is derived from the social media. I imagine that it would be best for the audit committee to have a response plan.

GL: I am in favour of the most precise policies and action plans for each of the major incidents foreseen. The response plans must be practical, cover various scenarios, because in general what happens is not what you are prepared for. The audit committees may check the procedures, but there is no way of foreseeing how to face the most serious possible risk type, and as this is a sensitive issue I believe that it should be presented quickly at the board of directors level.

How can the audit committee ensure that the desired culture spreads across the whole organisation? What role can the committee play when it comes to analysing its work with the culture of the organisation?

MN: The board of directors sets the guidelines, but the audit committee is key as defender of ethical values, and we have to remind the committee what it must do if they deviate from the objective. Another thing that we can do is test and request that internal audit should analyse the ethical tone of management and whether this permeates the rest of the organisation, whether the rules of ethical conduct are spread. Internal audit can ensure that people really understand the corporate culture.

GL: I agree, and the audit committee can also talk in depth with internal audit on the best way of assessing the corporate culture. It helps us to understand whether the culture really impregnates all parts of the organisation. The business culture would arise as the final responsibility within the board. They are the ones that must assume this responsibility.

CT: There are clear processes that have to do with culture; and it is important that internal audit should be connected to the audit committee. Internal audit must tell us what they need to assess it.

Should there be specific committees to assess complex areas, to assess them better?

CT: I think so. Once we tried to address a specific aspect of risk and we tried it with a group of internal and external experts to assess it. It was not completely independent, but it was a very good experience to provide more specific attention to a complete risk.

MN: we created one specifically on security, and its findings were relevant in assisting our work.

GL: My experience is different. They asked us to create one on digitalisation and cyber-risk, but because of the size of the board, the number of existing committees, etc. we saw that it was not efficient, because all the members of the board were preoccupied about this issue and everything revolved around the same thing. So we resolved it with a seminar of experts for all the directors, to provide an objective vision and see how to address these risks. We must also look to support from internal audit and assess the quality of the work on these risks.

What can the audit committee do to help internal audit?

CT: Support them, of course, and ensure that they have sufficient resources and budget. They must be assisted so that the voice of internal audit is heard in the business.

MN: Of course, and they must be understood and we have to assure ourselves that they are independent, that their statutes are protected and that they are relevant; that people are aware of their value, and contribute actively so that the message of ethical governance is disseminated across the whole organisation.

GL: First, we must ensure that internal audit is well positioned in the organisation chart to support its independence. The conclusions of the reports must be followed, and the operating teams must consider the recommendations of internal audit. They have to recognise how grateful we are to work with internal audit.

*Summary prepared by the Spanish Institute of Internal Auditors based on the opinions expressed by those taking part in the panel discussion.
Man’s landing on the Moon was a moment of great inspiration for Michael López-Alegría, who was 11 years old when Neil Armstrong took his place in history, and who made Michael think about being an astronaut for the first time.

He began his military career in the US Naval Academy, where he also graduated in engineering, and specialised in aviation. After reading an article in the academy’s magazine by chance, on the astronauts who had graduated at the centre, he again turned his sights on space. After continuing in flight training school, he enrolled in the NASA entrance exams. A committee made up of eight astronauts and four executives allowed entry to those most qualified, following some tough physical and technical exams. Finally, in 1992 he became an Astronaut Candidate (ASCAN).

During his initial period at NASA, he and his colleagues (21 men, 3 women, 10 pilots, 5 scientists, 4 medical doctors, 5 engineers and a veterinarian) began to learn how a spacecraft operates and carried out flight operations with space simulators on aircraft, pressure and gas resistance tests, etc.

His first space mission was in 1985, following specific flight mode training (flight tasks, micro-gravity, assembly of a space station, assembly and recovery of a space telescope, etc.). The deployment of a spacecraft involves an extremely complex protocol of actions until after 8 minutes of flight the craft is 28,000 kilometres from earth and thus in orbit. At this point the astronauts dedicate themselves to scientific, maintenance and construction work on the space station.

In 2003, after its third and final mission, the Columbia crashed with seven members of the crew aboard, due to a series of technical failures. This made the third accident, after those of the Apollo I and the Challenger. How can improvements be made? Space research is an activity that involves a number of technical challenges that have to be addressed through a system of risk management.

NASA uses a fairly simple risk matrix, according to López-Alegría. One scale presents the probability that an event may take place, and the other the seriousness of the incidents. The most important ones are those with the highest probability and greatest impact. In some cases, the analysis leads to the production of an attributed risk matrix, for which there are risk control mechanisms in place (above all training, redundancy mechanisms for protecting the equipment, other redundancies, etc.).

Any aspect of risk management in NASA operates in a very similar way to that in any company. It is an activity that is carried out within a specific programme, although it depends on the institution. But it is not sufficient, explains López-Alegría.

That is why in the wake of the Columbia accident a higher independent technical authority was established that has to approve all the operations for each launch. Everything must be reviewed by this technical authority. It is a relationship of independence and risk assessment that López-Alegría compares in general terms to that of any other organisation. Its methodology is based on free access and consultation, as is the risk matrix, but this is not the case with the assessment of the different key risks for the space station.

Another aspect highlighted by the Spanish-American astronaut as necessary for a space mission to be a success is training. In fact, he says that he never felt he was really in danger during his missions, “although if I had been, it would have been my training that would have allowed me to respond. Applying knowledge, reading, practicing, thinking… Our work consists of problem solving, and we can only do that through training.”

What has Michael López-Alegría learned about life in space that has taught him something about life on Earth? “Space changes how you see things. You realise how important life, love, our planet are… You can’t see any frontiers in space, or wars, or problems… In the history of humanity only a few people have had the opportunity to travel in Space, but it represents such an important life experience that I am in favour of democratising it, as we are doing at the Commercial Spaceflight Federation, and allow many more people to fly to space, because I believe that it would make the world a better place.”

*Summary prepared by the Spanish Institute of Internal Auditors*
THE ATMOSPHERE THAT WE
HAVE EXPECTED
THE ATMOSPHERE
FORMACIÓN 2019
destapa tu talento

89 seminarios
24% de novedades
835 horas lectivas
Nueva sección: Data Science

ALINEADO CON EL MARCO INTERNACIONAL PARA LA PRÁCTICA PROFESIONAL DE LA AUDITORÍA INTERNA, CON EL MARCO DE COMPETENCIAS DEL IIA GLOBAL Y CON LA ÚLTIMA EDICIÓN DEL ESTUDIO COMMON BODY OF KNOWLEDGE

www.auditoresinternos.es
¿A su departamento de auditoría interna se le acumula el trabajo?

Somos una empresa especializada en las auditorías de contratos y gastos con el objetivo de detectar y cuantificar los riesgos relativos a las relaciones con los proveedores de su negocio.

Tanto nuestra tecnología como nuestra experiencia nos permiten trabajar usando Data Analytics, analizando el 100% de las Compras, optimizando las conclusiones, detectando incidencias y sentando las bases para la mejora de procesos, complementando así el control interno de las empresas.

www.acfyd.com - Telf: 910 020 110 - comercial@acfyd.com