ICQ
IRISH COMPLIANCE QUARTERLY
Summer 2017

THE RISE AND RISE OF FINANCIAL CRIME

AML: Under Further Scrutiny

Heads of Data Protection Bill 2017

Isolde Goggin

# AN ENFORCEMENT PERSPECTIVE

Analysing your AML Culture

UNFAIR TERMS & USE OF PLAIN ENGLISH

ACOI

# Contents



*ICQ is published by:*
The Association of Compliance Officers in Ireland (ACO I), Lower Ground Floor, 5 Fitzwilliam Square, Dublin 2.
T: 01 - 779 0200.
*Production Team:* ICQ Editorial Committee and ACOI Executive. *Editorial and Production:* Intrepid Media Ltd.

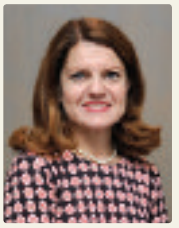
# WELCOME to the SUMMER 2017 Edition of ICQ


As ever, it has been a busy quarter for ACOI, one highlight (for myself anyway) was the Dinner in Clontarf Castle on 7th April. A very special venue, great food and brilliant entertainment made for a wonderful evening. I hope the members who attended enjoyed the evening, and you can try to pick yourself out in the photos in our Gallery in this edition.

We are bringing you something of an AML special this edition, starting with a very different outlook on financial crime - looking at reasons why individuals engage in financial crime. Then we have an added perspective on culture, as opposed to strict compliance, based on a recent lunchtime seminar, and for those members who could not attend, I hope the article on the AML Cultural Diagnostic will be insightful. We round off with an AML Legislative update. There are, as ever, developments in other areas such as Data Protection – and we bring you updates in these areas too.

We are grateful to Isolde Goggin, Chairperson of the Competition and Consumer Protection Commission for writing for us in this edition. Working in regulation as we do, competition is not always at the forefront of our minds when considering e.g. a legislative proposal, but some regulation can impact on competition and the regulators / legislators do not always consider these in the rush to bring forward regulation. Isolde also makes suggestions how we as compliance officers can deal with Competition Law compliance.

All good things must come to an end and my time editing the ICQ is over as I take up other responsibilities and this is the last edition I will be on the Editorial Team. I had big shoes to fill when I took on the role from Valerie Bowen, who did fantastic work to establish ICQ, I have enjoyed the experience of editing the magazine and I am grateful to the ACOI Board for giving me this opportunity. I have been very ably supported by the ACOI Executive and the other members of the Editorial Board, and my job was made easier by the Working Groups, sponsors, students and others who produced such high quality articles for inclusion. I wish to thank you all and I look forward to seeing how the publication is taken forward – I am confident it is in safe hands.



Yours in Compliance,

**Kathy Jacobs**
***ACOI Director***
***June 2017*** ICQ

KPMG

# At the heart of business in Ireland

# CEO UPDATE

*"Many of you will be receiving exam results now, we wish you the best of luck."*

With the upcoming transposition of 4MLD and new legislation due, this edition has a focus on AML/Financial Crime which we hope you will find interesting and informative. With implementation of GDPR less than a year away, we have articles to assist you on Data Protection.

On Friday 7th April last, we hosted the ACOI Annual Dinner in Clontarf Castle. There was a great turnout on the night with over 200 people in attendance. We had plenty of laughs and entertainment on the evening with David Meade, he really did seem to get inside our heads as he promised! There are many photos included in this edition and in the Gallery section of ACOI website. The charity raffle raised €2,800 for our nominated charities, Capuchin Day Centre for Homeless People and The Peter McVerry Trust, both very worthy causes. Thanks to all of you who came and supported the charities and to all those who donated such generous prizes to the raffle.

On Thursday, June 22nd we have the Education & Careers evening in the Marker Hotel. Come and join us and hear about the education programmes available to you and from recruiters on the current market developments. We have more in our Building Blocks Series in August: Compliance planning and monitoring. This series of six workshops held throughout the year, continues to prove very popular and the format allows time for discussion and analysis of issues and an opportunity to interact with peers.

Our events would not be possible without the input from our substantial panel of contributors and speakers so we would like to thank all those who support us in developing and delivering these events. It is all done on a volunteer basis and a huge wealth of experience is shared with the member base. So again, thank you.

For those of you who are thinking about upskilling, enrolments for September programmes are open. You can start, or continue, your studies, to attain the LCOI, by enrolling on the Professional Certificate and Professional Diploma in Compliance. This programme is designed for those who work or aspire to work in a professional capacity in a compliance function and is designed to enhance your skills, judgement and ability to deal with practical issues in the management and practice of compliance.

For Data Protection, we recommend attaining the Certified Data Prevention Officer, CDPO designation by completing the Professional Certificate in Data Protection. This is an excellent opportunity for you to demonstrate that you have acquired knowledge, specialist skills and competence to support and advise your organisation in getting ready for GDPR and in managing data protection related reputational, compliance and financial risks. This is supported by practical events. The next is on 29th August, John Keyes, Assistant Commissioner – Head of Investigations in the Office of the Data Protection Commissioner, will discuss the ODPC's approach to investigations, their main area of focus and their key messages for senior management.

Many of you will be receiving exam results now, we wish you the best of luck.

As many of you know Kathy Jacobs has been involved in the production of ICQ since 2015. With her new role as Chair of the ACOI Technical Committee, Kathy is stepping back from the ICQ. We would like to thank Kathy for her commitment to the ICQ; her comments have always been insightful and informative and under her watch the ICQ has gone from strength to strength.

To conclude we have a date for your diary, the ACOI 2017 Annual Conference Friday, 10th November in the Westin Hotel. ICQ

**Evelyn Cregan,**
***CEO***

# COMPETITION LAW from an ENFORCEMENT PERSPECTIVE

**Isolde Goggin, Chairperson of the CCPC, explains the key principles of competition law and how to ensure your company remains compliant with the Competition Act 2002 and its subsequent amendments*(1)*.**

In October 2014, the Competition Authority and the National Consumer Agency amalgamated creating the Competition and Consumer Protection Commission (CCPC), an independent organisation with a 360-degree perspective on consumer and market issues. The CCPC's mission is to make markets work better for consumers and businesses through a broader insight into market issues, whether they relate to a failure to comply with competition law, consumer protection concerns or a combination of these factors.

The CCPC has a broad mandate, which includes enforcing competition and consumer protection legislation, informing consumers about their rights and assessing mergers. We also have a specific remit in relation to product safety and the regulation of grocery sector business relationships. For Compliance Officers and particularly those working in the financial sector, it is the CCPC's role in enforcing competition law that is perhaps of most relevance. Competition law seeks to protect both consumers and businesses by ensuring that markets function properly.

## What is competition law and what does it prohibit?

Competition benefits everyone; businesses, consumers and the economy as a whole. Buyers of goods and services (both individual consumers and businesses) benefit by paying less and having more choice and better quality. Generally, anti-competitive behaviour inhibits productivity, innovation and means poorer value for buyers of goods and services.


www.ccpc.ie

Both Irish and EU competition law prohibit businesses from entering into anti-competitive agreements or concerted practices with other businesses. It is important to be aware that this applies not only to formal agreements but also to any sort of informal arrangement between businesses - whether written or verbal - which has an anti-competitive intention or effect. Both Irish and EU competition law also prohibit "abusive" practices by a business which holds a dominant market position. There are many types of practices and behaviours which may constitute a breach of competition law. As a Compliance Officer you should familiarise yourself with the main infringements of competition law such as price fixing, market sharing, bid-rigging and abuse of dominance. Agreements incorporating long exclusivity periods may also infringe competition law.

## What is a cartel and how can you identify a cartel in your industry?

A cartel is when two or more businesses agree not to compete with each other. This is the most serious form of anti-competitive behaviour. Cartels can result in increased prices, lower quality products and narrower choice for consumers. As a Compliance Officer, there are signs that you can look out for that might signal a cartel is operating in your sector. You might notice that competitors have agreed to price or discount products in a certain way, or that price changes happen regularly or follow a certain pattern over time. Alternatively, if a cartel has agreed to split the market then you may hear of refusals to provide quotes (or providing inexplicably high quotes) to customers outside their normal trading areas or comments from a salesperson that certain customers are "their customers".

*"A cartel is when two or more businesses agree not to compete with each other. This is the most serious form of anti-competitive behaviour."*

## Abuse of dominance and other anti-competitive agreements

Another possible contravention of competition law is where a dominant company abuses its position of power to stifle competition in a particular market. Compliance Officers across the economy should be aware that certain commercial practices could be considered an abuse of dominance; these include predatory pricing, exclusivity arrangements and fidelity rebates. More specific examples of the impact of anti-competitive behaviour include;

**Abuse of Dominance arrangements are:**

- Predatory pricing: this is when a business prices a product or service below cost with the intention of driving competitors out of the market, or preventing new competitors from entering the market.
- Exclusive dealing: this is when a business requires a customer to purchase all their requirements exclusively from that organisation. This may result in the consumer paying above average price for a product or service. If the consumer in this instance is a business it can lead to significantly higher over heads and a subsequent reduction in profit.
- Fidelity rebates: this is when a business offers rebates to a customer conditional upon them purchasing exclusively form that organisation. This can have a negative impact on other market practitioners as it effectively removes them from the competitive process.

**Collusive tendering can result in:**

- Consumers being deprived of the benefits of competition, enabling businesses to earn higher profits for less effort.
- Collusive tendering generally means that the procurer, pays more for goods and services than they would in a truly competitive situation. It also often means that the procurer receives poorer quality goods and services as tendering parties don't have an incentive to provide quality services.
- Firms involved in collusive tendering also have less incentive to be efficient and innovative, and this ultimately raises the cost of doing business in the entire economy.


## What should a Compliance Officer know about sharing information with competitors and competition law?

Perhaps the most important principle of competition law for any Compliance Officer to understand is that competitors are required to act strictly independently of each other in any market. When two or more competing companies share commercially sensitive information - whether directly or indirectly through a third party - this can cause two types of problems.

First, exchanges of commercially sensitive information may facilitate collusion between companies participating in the information exchange, enabling those businesses to engage in cartel activities such as price fixing, market sharing, limiting output, and bid rigging. Second, even in the absence of cartel activity, an information exchange mechanism may still fall foul of competition law if it increases market transparency to such a degree that companies are aware of their competitors' future intended behaviour on the market. This may reduce their incentives to compete and lead to competition on the market being prevented, restricted, or distorted.

## Factors to consider when exchanging or sharing information

While companies may seek to exchange or share information for legitimate business reasons, any exchange of commercially sensitive information between competitors is likely to interfere with the normal conditions of competition in their particular market. As a Compliance Officer, you should assess whether an information exchange has the potential effect of restricting competition in a particular market.

In order to do this, it is necessary to take into account all of the circumstances in which the information exchange takes place - including the type of information that is exchanged, the method by which it is shared and the characteristics of the relevant market more generally.

The nature of the information that is to be shared with your competitor is of key importance for determining whether the information exchange may have the effect of restricting

competition in a particular market. The CCPC considers the following types of information to be commercially sensitive and, in most circumstances, this type of data must not be shared between competitors:

1. current and future pricing information (for example, actual prices, discounts and rebates)
2. current and future output and sales information (for example, volumes, turnovers and market shares)
3. current and future commercial plans (including, product development, marketing and promotional plans)
4. information about costs and
5. customer lists.

This list is not exhaustive and there are other types of information (e.g. distribution channels) which have the potential to be commercially sensitive depending on the circumstances of the information exchange.

## How we enforce competition legislation

The information provided to the CCPC by consumers, businesses, other Irish regulatory bodies and our European and international colleagues forms the basis of much of our enforcement work. We also undertake our own market surveillance and information gathering. If there is sufficient evidence, we may then open an investigation and, where we find that a business has broken the law, we will take appropriate enforcement action to address the harm caused.

We actively encourage any individual who believes that they have information about a potential breach of competition law to contact us. An important tool that we use in our detection of cartels is our Cartel Immunity Programme ("Programme"), which we operate in conjunction with the Director of Public Prosecutions (DPP). The Programme means that a member of a cartel may avoid prosecution, including fines and jail time, if they are the first member to come forward and reveal their involvement in illegal cartel activity before the CCPC has completed any investigation and referred the matter to the DPP. Under the Programme, the CCPC acts as an intermediary between applicants and the DPP in seeking immunity from prosecution in return for providing evidence in a criminal trial.

## Consequences of breaching competition law

At the conclusion of any competition law investigation, we may opt to take either civil or criminal action against the company and/or any individual concerned. Where we consider the matter to be civil in nature, we can

initiate civil proceedings in the courts against the company or individuals.

If we believe breaches to be criminal in nature we have powers to prosecute in the District Court. For more serious breaches of competition law such as price fixing or bid rigging, we may send a file to the DPP who will decide whether to bring a prosecution on indictment in the Central Criminal Court. There are strong penalties set out in the Competition Act 2002 for those found guilty on indictment.

A company can be fined up to €5 million or 10% of their annual turnover, while an individual can be fined up to €5 million or 10% of his or her annual turnover and can be imprisoned for up to 10 years. For example, in 2012, members of a home heating oil cartel were convicted of price fixing ***(2***). Two members of the cartel received suspended custodial sentences from six months to two years respectively, while all convicted members of the cartel received a fine of between €1,000 and €30,000.

## Our enforcement priorities

Cartel detection, particularly bid rigging in procurement, is a particular priority for us because it causes the greatest harm to consumers. We have a case currently before the courts, where an individual and a business have pleaded guilty to engaging in bid rigging in the commercial flooring sector. Recently, we also confirmed an ongoing investigation into potential bid rigging in the procurement of publicly funded transport services.

We are also very active in taking enforcement action against firms engaging in anti-competitive information sharing and other anti-competitive agreements.

Last year, we opened an investigation, which is ongoing, into potential price signalling within the motor insurance market. We also concluded two investigations which resulted in the CCPC obtaining legally binding commitments from the businesses under investigation – one which related to information sharing between private motor insurers via a software product provided by a software company, Relay, and the second which related to the publication of minimum pricing guides by a trade association.

In January 2017, we also concluded an investigation into potential anti-competitive conduct by the Irish Property Owners Association. The investigation related to whether the IPOA had attempted to co-ordinate the business conduct of its members. To address the CCPC's concerns, the IPOA gave a number of legally binding commitments regarding its future conduct.

## How to help your business to comply by introducing a compliance programme

It is vital that a culture of compliance is encouraged throughout your business and that there are sufficient internal policies to support adherence to the highest professional standards of compliance with competition law. This should be evident from the top levels of management down through all levels within the organisation. Adopting a competition law compliance programme is the best way you can help your business to have the right measures in place and it should form part of your company's overall risk management and compliance procedures.

Every business needs to design a compliance programme that suits its needs. It will depend on the structure and conditions of the market you are operating in and the size and structure of your business.

A compliance programme need not be costly but should be implemented fully, with proper training for staff and reviewed regularly. Once staff are trained, they will also be able to identify instances where your firm is a potential victim of an anti-competitive practice. It is important to be cautious and where there is any doubt about an information exchange, a proposed agreement or any other aspect of your company's conduct consult with your legal advisors. ICQ

***More information about competition law and our investigations can be found at www.ccpc.ie.***

***Isolde Goggin is Chairperson of the CCPC***

*Footnote: 1. http://www.lawreform.ie/_fileupload/RevisedActs/WithAnnotations/EN_ACT_2002_0014.PDF (PDF Link to COMPETITION ACT 2002 REVISED Updated to 1 October 2015) 2. https://www.ccpc.ie/business/enforcement/criminal-enforcement/criminal-court-cases/home-heating-oil-cartel/*

THE SCIENCE BEHIND

# THE RISE & RISE OF FINANCIAL CRIME

**As he was being led to jail to begin his 24-year sentence (later reduced to 14 years) Jeffrey Skilling the former CEO of Enron was reported to have plaintively muttered "But I didn't hurt anyone!" Studies of other highly placed financial and corporate criminals show he may well have believed it.**

**THE ACOI is a founding member of the International Federation of Compliance Associations (IFCA). Another one of the four founding members was the Governance Risk and Compliance (GRC) Institute from Australia. In the spirit of sharing information and publications to assist members achieve a global perspective on common issues the GRC Institute has kindly allowed the members of ACOI access to this article. Behavioural finance, conduct risk and the importance of risk based cultures can be illuminated when the science behind the rise of financal crime is considered. The behaviours and justifications considered in this article are by no means exhaustive but act as a basis to consider crime through a scientific lens. The author Dr Bob Murray is a co-founder of the international consultancy Fortinberry Murray. Dr Murray works with Global 500 companies, Governments and major professional service firms in Asia, the US, Europe as well as Australia. He is the author of 10 books.**

Much recent research has shown that financial and other corporate crime originates, and is mostly perpetuated by, those at or near the top of the corporate tree. Their accomplices are often in the middle management of their businesses. Interestingly the psychic motivation—the behavioural neurogenetics if you will—of the two layers are quite different. As both a psychologist and a scientist in this area I find this fascinating. What makes otherwise "sane" men and women set out to rob and defraud their shareholders, their staff, and their customers?
The iron law of genetics is simple—if something is occurring frequently and has occurred frequently throughout recorded history it probably has a genetic base to it. Something in our DNA causes us act in an antisocial manner in certain contexts and under the influence of certain circumstances. It's a subject I have researched deeply and continue to do so. Since this is a short piece I'll concentrate on only three factors, my excuse is that they are the main ones and my mea culpa is I am leaving out many, many qualifications and other issues behind this kind of crime.

*"The medieval kings of Europe had it down to a fine art, they called it 'the divine right of kings.' You might rename it for modern times as 'The CEO infallibility complex.'"*

## Factor One: the Executive Bubble

Let's start at the top with the Skillings of this world. CEOs and others in the corporate "C" suite tend to inhabit what is called an "executive bubble." Those inside the bubble receive very little information from the outside—people feed them what they want to hear and anyway they aren't listening to anything that contradicts their own opinions. Anything that they do is justified by excuses stored in or framed by assumptions about themselves or their position within the brain's orbitofrontal cortex.

The medieval kings of Europe had this down to a fine art, they called it "the divine right of kings." You might rename it for modern times as "The CEO infallibility complex." Skilling believed that his position gave him the right to behave as he did and convinced himself that he was a perfectly moral being who "didn't hurt anyone." And anyway, if he did, it was their fault for being so stupid. In my interviewing of corporate criminals, I have heard this line so often. Sometimes followed by "Anyway someone should've stopped me!"

The DNA link here, I suspect, is in the genes that control the reward neurochemical dopamine. Once you have reached a certain point and you are earning millions a year there is nothing left to really excite or "reward" you. This lack of dopamenic stimulation makes you feel that you are being undervalued, especially when you compare yourself to those CEOs who are making more than you are. This justifies you in your own mind in making up for the lack by the modern equivalent of medieval "rape and plunder." In all cases the propensity to get caught in a bubble can be seen in the perpetrator's prior history but often boards (who are often in their own executive bubble) ignore evidence such as this when making their selection.

## Factor Two: the Testosterone Effect

Since a seminal study published in 2011 we have known that financial crime, like gambling and risk-taking, is closely linked to an elevated level of testosterone in the perpetrator's blood. From the same study, we also know that this is true of both men and women. It is linked to the inherited way that the genes controlling this neurochemical express themselves in an individual.

If a person has elevated levels of testosterone and finds themselves in a certain context—for example in a culture which favours risk-taking or financial crime (as in the banks and brokerages pre-2008) then they will probably be unable to resist the temptation to join in. Most of those who were involved in the massive fraud that took place at that time, and who were tested for one reason or another, were found to have greater than normal levels of testosterone in their system.

Recently, researchers have discovered close links between testosterone and psychopathology—a known marker for criminal and antisocial behaviour—and this has been definitively associated with financial and other corporate crime.

## Factor Three: Workplace Stress

Recent studies have shown that, particularly at the middle management levels, increasing stress and job insecurity have led to a great deal of financial crime. If a person is afraid of losing their job they will "take it out" on the boss, their fellow workers or their clients. Most often this takes the form of financial crime according to the 2014 Report to the Nations on Occupational Fraud. As workplace stress becomes more acute and as job loss and the threat of job loss becomes more pervasive, this factor will become more and more important.

Often financial crime by any individual can be a result of more than one of the above, but almost always one of them is in play.

There are solutions to all of these factors but often they require actions that businesses are reluctant to take because of a wide variety of, usually irrelevant, factors.

It often amazes me the lengths that firms and corporations will go to cover up the wrongdoings of their employees at all levels. But that is another story.

***This article was originally published in the Financial Crime 2017 Edition of the GRC Professional, which is a publication of the GRCI. The GRCI is the pre-eminent Australian-based professional association for compliance professionals. (www.thegrcinstitute.org/).*** ICQ

# Analysing your AML Culture

## FROM THE INSIDE OUT

**In 2013 Enterprise Ireland commissioned a University College Cork (UCC) research team to deliver a Capability Maturity Model for Anti Money Laundering (AML).**

An early review of the work by the then Head of Financial Regulation at the Central Bank of Ireland (Central Bank) challenged the team to find a credible way to assess AML Cultural Embedding. The AML – Cultural Diagnostic Tool emerged as output from that research. The Central Bank has continued its support of the UCC research, most recently inviting the UCC team to showcase its solution at the Central Bank's March 2017 bank briefing on AML supervisory engagement. This article explores the benefits of the AML Cultural Diagnostic (AML-CD) Tool.

In recent times regulators have increased their focus on the role culture plays in AML compliance. The UK's Financial Conduct Authority (FCA) annual report from 2013 stated that; "Without the right culture in a firm, it is unlikely that it will be able to embed an effective AML regime."

In 2014 the FCA said; "We found the failure to establish a good AML culture correlated strongly to poor overall AML and sanctions systems and controls." Similarly, FinCEN stated after 2013 that; "Shortcomings identified in recent AML enforcement actions confirm that the culture of an organisation is critical to its compliance."

Sylvia Cronin (Director of Insurance Supervision of the Central Bank) stated in her speech on culture at the 2017 ACOI AGM that "at the outset in 2016 we determined that cultural awareness would be an underlying theme as part of our normal supervisory activity." Similar references abound and include warnings from the Financial Stability Board in 2014 that "[regulators] should assess how the board and senior management systematically assess the risk culture of the institution," and from the G30 in 2013; "attention to risk culture must be a priority because it has the most direct connection to safety and soundness." In essence, regulators around the world now expect organisations to be able to demonstrate that they have periodically used a variety of formal and informal techniques to monitor risk culture ***(1).***

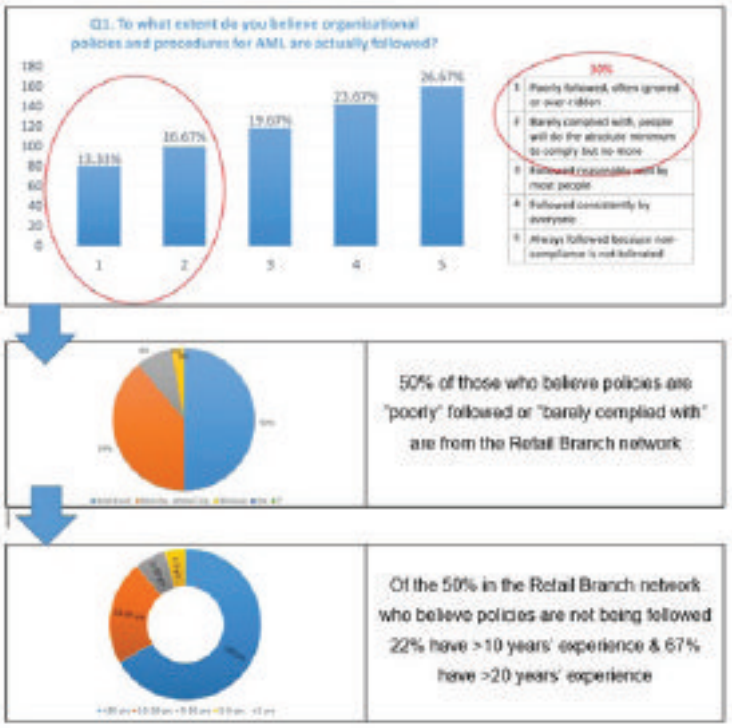
As compliance professionals, we all know and understand the requirements necessary to put the right AML processes in place. But how do you know whether those processes support and reinforce the right behaviour and culture? Organisations often fall into the trap of believing that once the right AML training and processes are in place then all the right behaviours will follow. Training and processes alone will not determine how your employees behave when under pressure and have to act instinctively.

### Assessing AML Culture

Organisations have tried a number of approaches to assessing AML culture. These include using psychologists who typically focus on the tone at the top and are therefore unable to reveal what the prevailing culture on the ground is. This approach makes no allowance for the very real issue of sub-cultures or middle management failing to disseminate the message into the first line of defence. It is therefore unlikely to identify a manager who is adept at easing staff into unethical practices by "normalising" non-compliant behaviours.

Other organisations have incorporated AML into the general assessment of

**Sample AML-CD Output for one Question**




Operational Risk. Again, while there are some merits in this, depending on how it is executed, AML will only be one component of the overall Operational Risk assessment and may not even include any assessment of specific AML concerns.

In short, some organisations have tried to assess AML culture by using staff surveys with questions posed and Likert scales (e.g. questions with 1-5 scale, 1 being the least, 5 being the most) presented for the selection of answers. These make no allowance for the subjectivity of the respondents e.g. Is one person's consideration of '3' the same as another person's '3'? These types of surveys are often only focused on organisational risk culture as distinct from a culture of AML compliance and risk awareness and lack the nuance of a model rooted in AML obligations.

Therefore, finding a means to effectively measure culture and actually finding a rapid, cost effective and thorough way to develop a documented understanding of the prevailing AML culture in any organisation has, to date, eluded everyone.

## Why is it so difficult to measure culture?

We know that "you can't manage what you can't measure" (Peter Drucker), so it's not unreasonable to assert that in order to manage culture you have to be able to 'measure' it. However, the real challenge is to find a reliable way to 'measure' such an intangible as AML culture, and to do so in a cost effective and rapid way. To meet this challenge the UCC research team adapted a framework that NASA uses to measure nebulous concepts like "quality" and found that the same methodology, GQM ***(2)***, could be applied to assess AML cultural embedding.

We extracted seven essential cultural embedding factors (leadership, policies, resources, training, rewards and recognition, ownership, & communications) identified in the AML Maturity Model ***(3)*** which is the most comprehensive AML model developed to date, and applied the GQM methodology to them.

> ***"Finding a means to effectively measure culture and actually find a rapid, cost effective and thorough way to develop a documented understanding of the prevailing AML culture, has, to date, eluded everyone."***

**Sample High Level Output for AML-CD**


**GQM defines a measurement model on three levels:**

- **Conceptual level (Goal):** This is the highest level and asks what Goal does the business want to accomplish? In our case it is to understand the extent of AML cultural embedding within an organization.
- **Operational level (Question):** As 'culture' cannot be directly measured we must determine what Questions we can ask to help us characterise the Goal and help our understanding of the extent to which the Goal is being achieved.
- **Quantitative level (Metric):** Each Question at the Operational level is assigned a set of Metrics enabling us to answer the Questions

*"Problems can be isolated and analysed from multiple perspectives thereby enabling the identification of specific issues or specific cultural embedding problems including sub-cultures and training deficiencies."*

based on factual data and thereby determine objectively if the Goal is being achieved.

We also worked with the applied psychology department in UCC to validate our choice and handling of both the seven cultural embedding factors and the questions and metrics asked throughout the diagnostic.

The end result is the AML Cultural Diagnostic (AML-CD), a repeatable, consistent, and rapid cloud-based survey instrument that assesses the views of not just the MLRO or management but of all employees in the organisation from the board down to front line staff. It is completely anonymous and takes approximately 15 minutes to complete. Problems can be isolated and analysed from multiple perspectives thereby enabling the identification of specific issues or specific cultural embedding problems including sub-cultures and training deficiencies. This data can be combined with participants' free-text comments to produce rich data-sets that give enormous insight into the prevailing AML culture.

## AML – CD Benefits

**The AML – Cultural Diagnostic:**

- Reduces AML compliance risk by rapidly and cost effectively identifying where cultural strengths and weaknesses exist and whether your people, processes and technology adequately reinforce the AML culture you want to create.
- Is quick, easy to use and cost effective.
- Delivers concise reports evidencing that a cultural assessment was conducted for regulatory engagement purposes.
- Accelerates cultural remediation planning and re-design.
- Enables the organization to establish its own internal benchmarks and identify any trends and changes in its AML culture or alternatively to benchmark itself against other organisations in the same industry.

The AML-CD can be paired with the AML-Performance Diagnostic (AML-PD) which enables a critical self-assessment of an organisation's own AML framework. The combination of the two diagnostics provides a complete AML process and cultural picture.

UCC has commercialised the AML-CD and AML-PD diagnostics through Durrus Compliance Diagnostics, a UCC spin-out company. permanent tsb rolled out both diagnostics in May 2017 and the output reports were delivered by Durrus Compliance Diagnostics at the end of May 2017. Bank of Ireland is rolling out both diagnostics in early June.

***Tara Casserly, Researcher UCC, & Director of UCC spin-out company Durrus Compliance Diagnostics & Mairead Kirwan, Head of Financial Crime Compliance & Group MLRO at permanent tsb.*** ICQ

**In the next AML article (page 18), Niamh Lambe, Director & AML Specialist, KPMG, provides a commentary on further developments in AML, making reference to this cultural diagnostic tool**

***1.*** *G30 2013.* ***2.*** *GQM, Goal, Question, Metric, is an approach to software metrics that has been promoted by Victor Basili of the University of Maryland, and the Software Engineering Laboratory at the NASA Goddard Space Flight Center. (https://en.wikipedia.org/wiki/GQM).* ***3.*** *The AML Maturity Model (AML-MM) was developed by the UCC team and is a multi-jurisdictional enterprise wide Capability Maturity Model that can be used as part of deep dive assessments to determine AML effectiveness.*

# Unfair Terms & Plain English in Consumer Documentation

**Neither the Unfair Terms Regulations (UTR) nor the regulatory focus on using plain and easily understood language in consumer contracts is new, but both have become the subject of greater court and regulatory focus recently.**

The UTR seeks to protect consumers against terms causing an imbalance in the parties' rights and obligations under a contract to the detriment of the consumer and are particularly focused on pre-printed standard form contracts. Any terms violating the UTR are unenforceable and may be set aside by a court. Up to recently, there has been little commentary from the Irish courts on the UTR. However, two recent cases - *AIB v Counihan* ***(1)*** and *Grant v Laois County Registrar* ***(2)*** have shone a spotlight on this area. In *Counihan*, the court declined summary judgment on a business loan, accepting the borrowers' claim that they were, in fact, acting as consumers which met the burden for plenary hearing. *Counihan* suggests that there is a positive duty on the court, to assess a contract for unfair terms, whether or not the borrower has raised a UTR issue. *Counihan* has the obvious potential to make it more difficult for financial institutions to enforce lending contracts, making its outcome one to watch.

*Grant* involves the judicial review of a County Registrar (CR) decision that failed to consider if a mortgage complied with the UTR, despite the CR (like the Financial Services Ombudsman (FSO)) not having jurisdiction to assess contracts for UTR compliance. Notably, in *Grant*, the case was funded by the Open Society Justice Initiative, which has supported similar cases in Europe. As the CR deals with residential mortgage enforcement cases, *Grant* raises questions over whether the CR's jurisdiction is open to challenge if they do not have jurisdiction to assess contracts for UTR compliance. Both *Counihan* and *Grant*, if successful at full hearing, raise the spectre of courts assessing loan and mortgage contracts for UTR compliance in all consumer enforcement cases, even where the issue is not raised by the borrower. This trend in Ireland follows a trend in Europe where the scope and application of the Unfair Terms Directive ***(3)*** has been broadened to protect consumers where possible and in all types of agreements, including personal guarantees and recent decisions are evidence of this ***(4)*** ***(5)***.

Although, there has been little specific regulatory guidance from the Central Bank on the UTR, the Central Bank has embraced the concept of plain English for some time, through requirements in the Consumer Protection Code (CPC). More recently, the 2016 CPC Addendum requires clear, consumer friendly, plain English drafting in Variable Rate Policy Statements and additionally consumer testing to ensure content is clear and easily understood.

The Central Bank commentary in press releases and the 2016 Consumer Outlook Report, make it clear the Central Bank is focusing on the UTR. In a UK context, the FCA has provided plenty of guidance on unfair terms and may review and make recommendations to firms on making terms more consumer friendly.

The impact of the preliminary decisions in *Counihan* and *Grant* remains to be seen, however, the outcome of both cases will be watched closely by lenders, given the potential for court scrutiny of all contracts in enforcement cases going forward. New and existing standard form consumer contracts including guarantees should also be scrutinised carefully for UTR compliance.

***Orla O'Connor, Partner, Arthur Cox and member of the ACOI Consumer Protection Working Group & Kim O'Dowd, Associate, Arthur Cox.*** ICQ

*(1) Allied Irish Banks PLC v Peter Counihan and Mary Counihan (HC)[2016] IEHC 752.* ***(2)*** *Grant & anor -v- Laois County Registrar (2016/787 )(JR)* ***(3)*** *www.ec.europa.eu/consumers/consumer_rights/rights-contracts/unfair-contract index_en.htm* ***(4.)*** *Aziz v. Caixa d'Estalvis de Catalunya, Tarragona I Manresa (C-415/11) [2013] 3 CMLR 89* ***(5)*** *Tarcău v Banca Comercială Intesa Sanpaolo România SA and Others (C 74/15) [19 November 2015]*

# AML and COUNTER-TERRORIST FINANCING

## UNDER FURTHER SCRUTINY


**With the fourth Anti-Money Laundering and Counter Terrorist Finance Directive (4AMLD) coming down the tracks, Niamh Lambe looks at what impact the new legislation will have on a wide range of financial and other institutions falling within the scope of 4AMLD (obliged entities), which include banks, investment funds and gambling entities, and what other AML/CFT developments obliged entities should have on their radar.**

## 4AMLD: What's involved?

The new legislation is designed to reinforce and expand on existing obligations imposed by 3AMLD. It puts the risk-based approach absolutely at the centre of tackling money laundering with a particular focus on the prevention of terrorist financing. Obliged entities should bear in mind that they must not only assess the risks that money laundering and terrorist financing (ML/TF) present, but must also document their methodology and rationale for their approach, including why it is appropriate for their specific business model.

*"The new legislation puts the risk-based approach absolutely at the centre of tackling money laundering with a particular focus on the prevention of terrorist financing."*

**The key changes within 4AMLD include:**

- **Beneficial ownership register:** Obliged entities will be required to maintain a register of the beneficial owners of their clients. This information will also be held in a central beneficial ownership register which will be managed by the Companies Registration Office (CRO). The change will help in identifying individuals behind shell companies, nominees and bearer instruments that the obliged entity does business with.

- The **automatic entitlement to apply Simplified Customer Due Diligence (SCDD)** is removed. The use of SCDD must now be justified on the basis that the business relationship or transaction carries a lower degree of ML/TF risk. Customer risk assessments are therefore likely to come under greater regulatory scrutiny.

- **Enhanced Customer Due Diligence (ECDD)** will be applied in more circumstances. Rather than maintaining a "white list" of equivalent jurisdictions, the EU Commission will identify high risk non-EU countries with strategic deficiencies in their AML/CFT regimes (the "**blacklist**"), which will require entities to apply ECDD to customers based in these countries. This will lead to an increased focus and reliance on an entity's country risk assessment. **Domestic Politically Exposed Persons (PEPs)** are now in scope for ECDD, whereas previously only non-domestic PEPs were subject to mandatory ECDD.

- The **scope of the Directive** has been extended. For example the threshold level for high value goods dealers to conduct customer due diligence has been reduced from €15,000 to €10,000 and applies to either payments made or payments received in cash.

The European Supervisory Authorities (the "ESA") has published guidelines on the factors entities should consider when assessing ML/TF risk associated with a business relationship and how to adopt a risk sensitive approach to performing Customer Due Diligence (CDD). As noted above, with the changes to ECDD and SCDD, customer risk assessments will become even more important and the ESA guidelines should be considered by entities in meeting their obligations.

## 4AMLD: Irish Update

4AMLD is meant to be transposed in EU Member States by 26 June 2017. Although the legislative process in Ireland is in train, with a consultation paper issued in January 2016 and the publication of a draft Head of Bill the (Criminal Justice (Money Laundering and Terrorist Financing) (Amendment) Bill) in December 2016, a revised Bill is due to be issued shortly and as the legislation has not been finalised, 4AMLD will not be transposed in Ireland on time.

Notwithstanding the delay, there have been two developments in terms of the Irish legislation which are noteworthy:

- An important amendment to the legislation has been agreed. The reference to a customer, where a customer means "the underlying investor in the fund" in the context of a fund service provider's business, is likely to be removed from the revised Bill as the fund service provider's customer relationship is with the fund rather than the underlying investor; and
- The beneficial ownership requirements have already been partially transposed into Irish law with the enactment of S.I.

560 2016 European Union (Anti-Money Laundering: Beneficial Ownership of Corporate Entities) Regulations 2016 in November last year. The early implementation was to enable obliged entities time to gather the necessary beneficial ownership data in advance of the national central register being established. It is anticipated that a statutory instrument will be published shortly to give effect to this register and to give an indication of how the register will operate. The requirements relating to the identification of the beneficial owners of trusts are still outstanding.

Whilst there are still some areas where clarity is required, for example the meaning of a "domestic PEP", the draft legislation issued to date, the consultation paper and the ESA Guidelines provide obliged entities with a good view of their future obligations.

## Impact of Technology

Technology innovation in financial services is top of the agenda, bringing substantial commercial benefit along with new unfamiliar risks to be managed including AML/CFT related risks. As technology has introduced new payment products and services to the financial marketplace, it has also introduced new potential avenues for individuals to commit ML/TF offences. These new payment methods such as mobile banking, mobile payments and virtual currencies bring many commercial benefits but also new risks of ML/TF. Such risks include:

- The potential for **anonymity** through the establishment of non-face-to-face business relationships, and consequently the reduced ability to effectively trace transactions as the relevant parties are not appropriately identified.
- The demand for real-time payments poses an **increased risk for fraudulent transactions** as there is less time and resources to fully scrutinise transactions.
- Other **common ML/TF risks** e.g. fictitious information, structuring of transactions, rapid transfer of funds are **intensified** through the use of technology.
- **Cyber attacks** provide opportunities to create vulnerabilities and bypass AML measures.

While obliged entities must recognise and be prepared for these emerging risks, they should also utilise technology to assist in enhancing their AML/CFT frameworks to meet their obligations and reduce the risk of money laundering and terrorist financing occurring. Deploying technologies strategically in the end to end process can not only reduce cost but also enhance the controls in place and reduce the level of AML/CFT risk in an organization. This can be seen at the crucial customer onboarding stage where technology solutions can align digital footprints with ID documentation and facial biometrics to support customer verification. Web-based solutions that deliver a comprehensive, automated risk-based profile of an institution's products, services, geographies and customer entities through a platform have also been developed. Other software tools are available to combat TF by screening watch lists in a systematic way.

Technology can also assist in the capturing and profiling of an entity's AML risk culture and behaviours, which so far has proved a challenging concept. With an increasing regulatory focus on "AML effectiveness assessment", entities are required to demonstrate that both their processes and equally their risk culture are delivering the right results and behaviours throughout the organisation. An "AML Cultural Diagnostic" tool has been developed by UCC researchers which focuses on AML behavioural strengths and weaknesses with the outputs of the tool identifying areas requiring AML compliance remediation. The tool provides a useful means to demonstrate to regulators that an appropriate AML culture is at the forefront of an entity's compliance agenda. The previous article in this edition titled, "Analysing your AML Culture from the Inside out" discusses the AML Cultural Diagnostic in greater detail.

## AML/CFT: Under Scrutiny

At a time when the requirements on obliged entities are more demanding and the risks of non-compliance are more prevalent than ever, the authorities responsible for supervising and enforcing AML/CFT are gearing up to meet their responsibilities.

**Financial Intelligence Units (FIUs)**
4AMLD contains new provisions to enhance co-operation between FIUs, to facilitate the exchange of information between them and to allow them to identify holders of bank and payment accounts. In Ireland the Garda Síochána's FIU will operate and monitor a new system - goAML - which will assist it to meet these new requirements. The goAML software application,

developed by the United Nations Office on Drugs and Crime (UNODC), was designed to provide a uniform and standard platform for combatting ML/TF by assisting countries in meeting international standards. In a nutshell, the goAML facility is an online reporting platform which facilitates the submission of suspicious transaction reports (STRs) from obliged entities. goAML operates on the basis of data collection, providing a secure web-based interface between FIUs and obliged entities, where STRs are assessed for completeness and accuracy. The STRs will be analysed to identify trends and patterns in ML/TF, to assign tasks and to monitor progress. It also provides the FIU with a template for producing a final report on a case for dissemination to other FIUs. Obliged entities have been able to register and file STRs on the new system since 12 June 2017.

**Central Bank of Ireland (Central Bank)**

Over the past few years the Central Bank has used its Risk Evaluation Questionnaire (REQ) to assess obliged entities' exposures to ML/TF risks and their ability to monitor these risks. The REQ provides a mechanism for collating information such as:

- A breakdown of products and services offered by a firm.
- Distribution channels utilised by the firm in relation to the products and services it offers.
- Details of products or services being "passported" out to other EU Member States.
- Customer exposure.
- Details of the firm's screening processes in relation to politically exposed persons (PEPs) and financial sanctions (FS).
- The implementation of the firm's AML/CFT policies and procedures.
- Whether the firm has an assurance testing programme.
- Details of any reliance placed by the firm on third parties.
- Whether the firm outsources any AML/CFT functions.

Until recently the REQ was a paper-based return submitted by firms to the Central Bank on request. The REQ will now need to be submitted via the Central Bank's Online Reporting System (ONR). As before the Central Bank will select a number of firms to submit an REQ, which will have to be submitted via the ONR and within a timeframe specified by the Central Bank. The Central Bank has published detailed information on the completion of the REQ and on how to access and submit the REQ via the ONR.

**Financial Action Task Force (FATF)**

Ireland's last Mutual Evaluation Report (MER), which was carried out in 2006, saw it assessed as being partially compliant with the FATF recommendations and it was placed into a follow-up process, which lasted a further seven years. By June 2013, FATF acknowledged the significant progress made by Ireland in addressing the deficiencies which were identified in 2006 and removed Ireland from the follow-up process.

FATF commenced its fourth round of MER in 2014, with a review of Ireland taking place in Q4 of 2016. FATF intends to discuss the findings of its review of the Irish AML/CFT system at its June 2017 ***(1)*** plenary meeting at which point it will determine whether Ireland should be placed in "regular" or "enhanced" follow-up. If Ireland is placed in regular follow-up, which is the default monitoring mechanism for all countries, then it will have its next follow-up in five years. If the FATF determines that there are significant deficiencies, then the follow-up process will be much more intensive.

**European Commission (EC)**

Following recent terrorist attacks in Europe and the Panama papers controversy, the EC has already proposed an amendment to 4AMLD to further reinforce EU rules to combat terrorist financing and increase transparency of financial transactions and corporate entities. The proposed amendment, commonly referred to as 5AMLD, is yet to be ratified and is currently at trialogue stage in the EU legislative process. If agreed, 5AMLD will supersede certain elements of 4AMLD and has a proposed implementation date of six months after publication of the Directive, which could potentially be towards the end of 2018.

AML/CFT will continue to preoccupy obliged entities into the future as the requirements become more demanding and the threats of ML/TF increase and as the ability of regulatory authorities to monitor them is enhanced.

***Niamh Lambe, Director & AML Specialist, KPMG*** ICQ

***(1)*** *http://www.fatf-gafi.org/calendar/assessmentcalendar/?hf=10&b=0&s=asc(document_lastmodifieddate)&table=1 (FATF assessment calendar)*

# DATA'S GAME CHANGER

**Denis Kelleher writes about the the General Data Protection Regulation (GDPR), one of the most important pieces of legislation ever to be introduced in Europe.**

Helen Dixon, the Data Protection Commissioner, has described the application of the General Data Protection Regulation (GDPR) as "a game-changer for citizens and businesses across Europe". The GDPR will apply from 25th May 2018 and will have direct effect as it is an EU Regulation. Hence the GDPR is going to apply to Irish data controllers, processors and subjects regardless of what Ireland or any other Member State does.

However, the GDPR does contain a wide variety of provisions that may be adapted by Member States. It also requires that the powers and functions of the Data Protection Commissioner be significantly enhanced.

In addition, the new Data Protection Directive, which applies to the processing of personal data in the criminal justice sector, must be implemented by 6th May 2018. This also requires national legislation. And so, Frances Fitzgerald, Tánaiste and Minister for Justice, on 12th May 2017 has published the General Scheme or "Heads" of the forthcoming Data Protection Bill 2017. The General Scheme (Heads) is considering the implementation of both GDPR (Regulation) & the Data Protection Directive.

The Heads have been approved by Cabinet. This means that they can now form the basis of instructions to drafters in the Office of Parliamentary Counsel who will now turn the Heads into a Bill. The Heads may also form the basis of Pre-Legislative Scrutiny, which is a process whereby the Heads may be considered by an Oireachtas Committee before the drafting of a Bill is finalised. Once the drafting is finalised the Bill will go to Cabinet for approval, before being formally introduced and then debated by the Oireachtas. The time for completing this work is short, but the GDPR will apply on 25th May 2018 regardless of whether the Oireachtas enacts this Bill.

The Heads do not propose the repeal of the existing Data Protection Acts. These will remain, though as the Heads point out they will largely be superseded by the GDPR and provisions of the Data Protection Bill 2017 that give effect to the new Directive.

Some may argue that it would be better to have a single data protection law but that is not possible. When the GDPR was originally proposed back in 2012 it had been hoped that it would provide such a single law. But as that proposal made its way through the EU's legislative process it gathered a variety of provisions that required or permitted Member States to introduce national implementing measures. In addition, there are some activities that will fall outside the scope of the GDPR and the new Directive, and some national regimes have to remain in place for such activities. Hence the existing Data Protection Acts may remain on the statute book, although it will be of limited application.

The modernisation of the DPC's Office is one the Head's most noteworthy features. This Office is to be re-established as a Data Protection Commission (DPC), with three members, including a Chair. This DPC will be the State's Data Protection Authority for the purposes of the GDPR and as such is required to be independent by the EU Treaties and GDPR. And so, the DPC will have the power to appoint its own staff and determine their grades, subject to the approval of the Minister for Public Expenditure and Reform. Unlike other supervisory bodies such as Comreg or the Central Bank, the GDPR does not grant the DPC a power to independently fund itself though levies or fees. Instead the DPC will be funded from the Exchequer, though the Heads note that the mechanism by which this funding is to be provided has yet to be finalised.

***"What the Heads can do is make provision for "procedural safeguards" and "due process" when these powers are being exercised by the DPC ."***

Part 5 of the Heads makes some provision for the supervision and enforcement powers of the DPC. The actual powers of the DPC are set out in Article 58 of the GDPR. The Heads cannot propose to amend or vary these. What the Heads can do is make provision for "procedural safeguards" and "due process" when these powers are being exercised by the DPC. So, the Heads provide for the appointment of authorised officers, the issue of search warrants, information and enforcement notices. An interesting power, which some readers may recognise from the Central Bank (Supervision and Enforcement) Act 2013, is suggested by Head 73. This is the power for the DPC to require a

report to be provided by a person nominated by the DPC or the controller or processor in question.

One of the highest profile new functions of the DPC will be that of imposing fines. Interestingly, the Heads setting out the procedure by which these fines may be imposed are not modelled on the Administrative Sanctions (ASP) Regime set out in the Central Bank Acts. Instead they are modelled on what can be found in the Property Services (Regulation) Act 2011. Under this model such fines must be confirmed by either the Circuit or High Courts. The use of this model is not certain; the Heads note that it has to be further discussed with the EU Commission.

Whatever model is ultimately adopted in the Bill, it seems certain that the imposition of fines will give rise to significant work for the DPC. And one of the justifications offered by the Heads for creating a three person DPC is the administrative and procedural burden that will arise from the "possibility of stringent sanctions, including large administrative fines…" As the Heads explain the GDPR "… provides limited flexibility for Member States to enact national law to adapt certain of its provisions to the needs of their legal systems and public sectors" These adaptations are set out in Part 3 of the Heads. This Part allows for the State to set a "digital age of consent" though a decision on what this age is to be has yet to be made.

Provision is also made for the processing of criminal records, the processing of sensitive data where "necessary for reasons of substantial interest" and the making of regulations requiring the appointment of Data Protection Officers.

*"Other provisions to be found in the Heads include an offence of disclosing personal data obtained without authority together with the publication of sanctions and convictions that may be imposed."*

Two other provisions seem likely to attract most interest, however. One is Head 20 which "permits limited restrictions on controller/processor obligations and the exercise of data subject rights". The other is Head 23 which provides that fines may only be imposed "on a public authority or body in respect of an infringement… arising from its activity as an undertaking" This means that fines can only be imposed on public undertakings such as Dublin Bus that compete with commercial undertakings. This reflects the reality that a fine imposed on a public body such as a Government Department will simply amount to a circular transaction returning public monies to the Exchequer from which it came. Unfortunately, there is a real danger that this provision will be misconstrued as conferring some form of exemption on public bodies, which it does not.

Other provisions to be found in the Heads include an offence of disclosing personal data obtained without authority together with the publication of sanctions and convictions that may be imposed. Rules of Court may be amended to make specific provision for data protection actions. The Courts will get their own supervisory authority, a judge of the High Court.

The implementation of the new Data Protection Directive takes up Part 4 of the Heads. These impose obligations on "competent authorities" which are any public authority or other entity engaged in the prevention, investigation, detection or prosecution of crime. Part 4 provides: rules for the Collection, processing, keeping and use of personal data; security measures for that data; data quality; specific rules for the processing of sensitive personal data; the rights of data subjects and the imposition of restrictions upon those rights.

The Heads, the new Directive and the GDPR must be read side-by-side, with occasional reference to the existing Data Protection Acts. The EU is already considering other laws, such as the proposed ePrivacy Regulation that will only add to this complexity. All of this complexity must ultimately be interpreted by the EU's Court of Justice, which is bound to uphold data protection as an EU fundamental right. Understanding data protection law is already hard, the publication of these Heads is part of a process that will make obtaining that understanding even harder.

***Denis Kelleher BCL LLD is Senior Legal Advisor, Central Bank of Ireland and lecturer on Professional Certificate in Data Protection.*** ICQ

*Footnote: The reform of the EU's data protection rules began in January 2012, resulting in two key pieces of legislation, GDPR (Regulation) & a specific Directive (680/2016) on data protection in the area of police and justice. The General Scheme (Heads of Bill) is considering the implementation of both GDPR & this Directive.*

*Data Protection & Technology*

# A REVIEW

## OF THE 28th ANNUAL REPORT OF THE DATA PROTECTION COMMISSIONER

**The Annual Report (the Report) of the Office of the Data Protection Commissioner (DPC) was published on 11 April 2017. The Report highlights the activities of the DPC across all of its regulatory functions in 2016 and points to the DPC's priorities for 2017. The Report each year provides a valuable insight into the deployment of resources within the Office of the DPC, its key messages for data protection compliance, its approach to regulation and its engagement with industry on privacy related policies, products and services. The key trends arising from the 2016 Report include the following:**

### Increased Capacity

The DPC continued to prioritise its expansion throughout 2016 with the addition of three deputy commissioners. The Report notes a total increase to 61 staff members as well as the intention to recruit a further 35 staff in 2017 with its increased budget of €7.5m. Additional resourcing enabled the establishment of a formal Senior Management Committee within the Office of the DPC and a new Multinationals and Technology team at the DPC with specific responsibility for the supervision of and engagement with the plethora of multinational companies now based in Ireland.

### Rise in Complaints

The number of individual complaints received by the DPC continued to increase in 2016 to over 1,400 complaints. A marked increase, of close to 60% on the previous year, indicates the growing awareness of data protection issues in Ireland. As in previous years access rights formed the basis for the majority of the complaints received (56%) followed by direct marketing complaints. While the majority of complaints were resolved under the amicable resolution process provided for under s.10 of the Data Protection Acts 1988 & 2003 ("the Acts") 59 formal decisions issued in 2016.

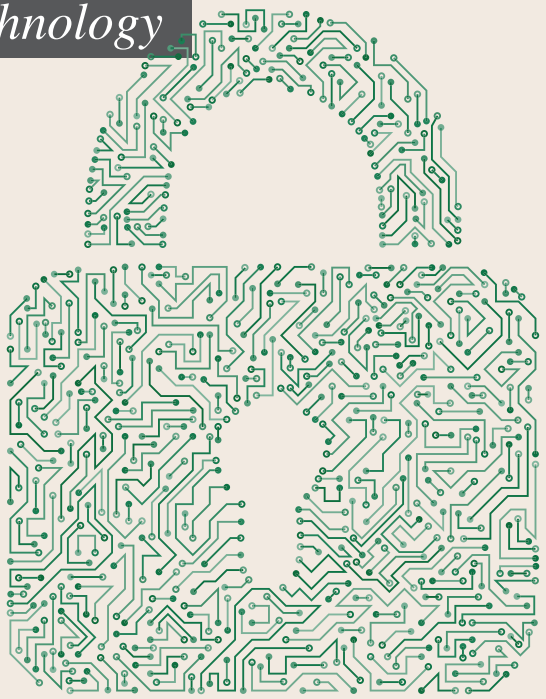
### Private Investigators

The initial focus of the Special Investigations Unit in the area of private investigators continued throughout its first year of operation with the successful prosecution of two private investigators for unlawfully obtaining and disclosing personal information to a third party. The investigation into this sector was also extended across all sectors using private investigators on a regular basis.

### Litigation

A centralised legal unit was established within the DPC in 2016 in order to support its other functions and to manage all litigation. Nine prosecutions were taken by the Commissioner in 2016 under the Acts and the ePrivacy Regulations. 2016 also saw the launch of an online judgments database to enable public access to written judgments and to increase awareness of developing privacy and data protection jurisprudence.

In the ongoing case of DPC v. Facebook Ireland Limited & Maximilian Schrems, the DPC has sought a reference to the Court of Justice of the European Union (CJEU) to examine the validity of standard contractual clauses. The hearing of this case took place over 21 days earlier this year and judgment remains reserved with no indication as to when it will



*"The Office of the DPC engaged with private and public sector organisations both nationally and internationally in 2016. "*

be delivered. The DPC also acted as a respondent or defendant in three other court proceedings in 2016.

## Data Breaches

In 2016 the DPC received 2,224 valid data breach notifications under the DPC Personal Data Security Breach Code of Practice. As in 2015, the majority of data breaches reported involved unauthorised disclosures such as postal and electronic disclosures, the largest number of which occurred in the financial sector.

One such case study described in the Report concerned a data breach by a named bank whereby personal data was disclosed to a third party when the data subject's old address was incorrectly linked to her new account. The data subject sought a formal decision of the DPC who found that the bank was in contravention of Sections 2A (1) and 2(1) b of the Data Protection Acts. The circumstances of this case accentuate the need to keep data complete, accurate and up to date at all times.

The inappropriate handling or disclosure of personal data by an unauthorised employee for example, the loss of personal data on smart devices, laptops and USB keys as well as an increase in network-security compromises such as ransomware and credit card scraping were listed in the Report as common data breaches reported to the DPC.

The effect of mandatory breach notifications under the GDPR on these figures will become clearer after the GDPR commencement date of 25 May 2018.

## Privacy Audits

50 in-depth audits and inspections were carried out by the DPC in 2016 to ensure compliance with the Data Protection Acts. Audits of private-sector entities included Allianz, VHI, Laya Healthcare, Meteor and Eir while under the Communications (Retention of Data) Act 2011 An Garda Síochána, the Revenue Commissioners, Defence Forces and Competition and Consumer Protection Commission were also examined. A number of best-practice recommendations were made in relation to prescribed agencies such as the need for the publication of disclosure policy and procedure manuals and to cite relevant legislation in all disclosure requests.

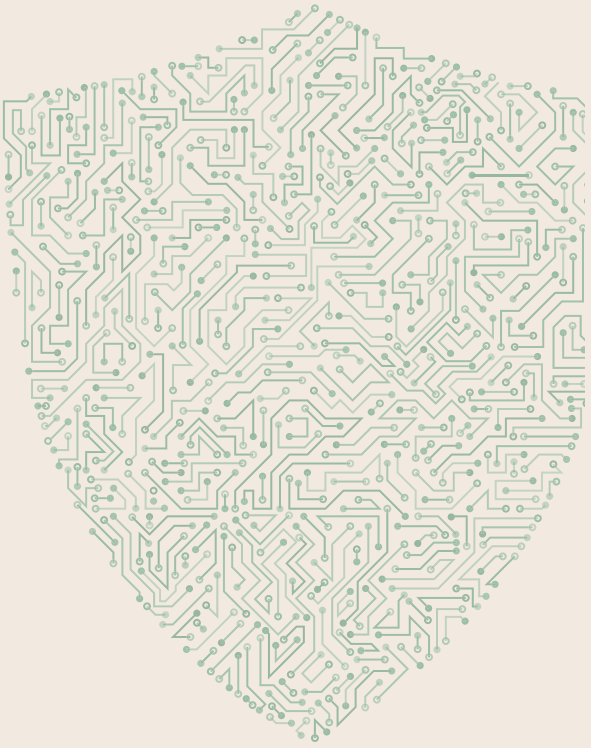
The audit findings and case studies in the Report highlight the shortcomings of many organisations' data security and retention practices with common failures to ensure that individuals are adequately notified of how their data is processed. The Report points to the increased need for modern, fit for purpose legislation and increased awareness of legal obligations.

## Engagement

The Report demonstrates the enthusiastic approach to engagement with stakeholders that has been adopted by the DPC. The Office of the DPC engaged with private and public sector organisations both nationally and internationally in 2016. The DPC engaged with the European Data Protection Supervisor initiative to promote co-ordination between European regulators and with the media and various

other public platforms to build awareness of data protection issues.

There was a particular emphasis throughout the Report on engagement by the newly formed Multinationals and Technology team. In attendance at over 100 face to face meetings with multinational companies, the DPC engaged in a review of both Apple's education service and changes to Google's terms, as well as its approach to online behavioural advertising. In consultation with the DPC, both Facebook and LinkedIn updated the information provided to online users regarding the use of cookies on their sites. Following the merger between Facebook and WhatsApp the DPC engaged directly with both entities to address their terms of service and privacy policy.



## GDPR

An increased focus on engagement coincides with the countdown to the introduction of the General Data Protection Regulation on 25 May 2018. It promises comprehensive transformation for data controllers and processors, including the numerous multinationals with their 'main establishment' in Ireland. The DPC emphasised the need for cooperation in relation to the one-stop shop model and the importance of quality controls and Privacy by Design under the GDPR.

The role of the DPC will change as part of Ireland's implementation of the GDPR. On 12 May 2017 the Tanaiste and Minister for Justice and Equality along with the Minister of State for Data Protection published the General Scheme of the Data Protection Bill. This includes a proposal to extend the suite of powers and tasks of the DPC to reflect the requirements of the GDPR.

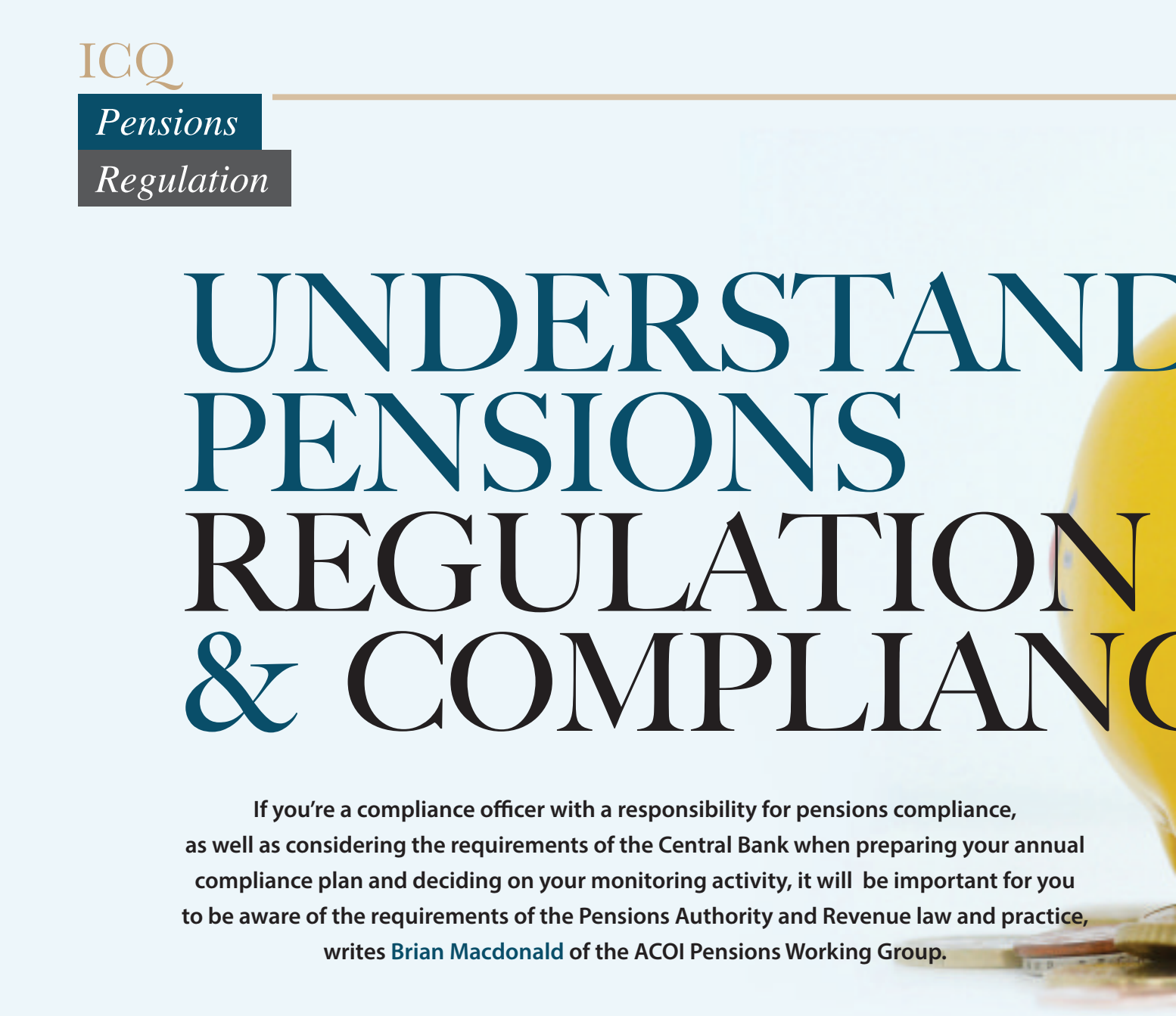
***Rob Corbet, Partner Arthur Cox, Member of ACOI Data Protection and Technology Working Group. With thanks to Ciara McDermott for her assistance in preparing this article.*** ICQ

***Footnote:*** *On Tuesday, 29th August 2017, the ACOI will host a Data Protection Seminar in Chartered Accountants House, 47-49 Pearse Street, Dublin 2. The theme is "Office of the Data Protection Commissioner (ODPC: Key messages on Investigations" and the speaker will be John Keyes, Assistant Commissioner – Investigations, Office of the Data Protection Commissioner. Some of the topics that will be discussed on the day include:*

- *The balance between a risk-based and complaints-led investigation approach;*
- *The ODPC's main areas of investigation focus;*
- *What firms can expect in terms of how an investigation is conducted; and*
- *Examples of the good and the bad the ODPC sees in terms of DP practice.*

The Seminar will be chaired by Aisling Clarke, Director ACOI and Chair of ACOI's Data Protection & Technology Working Group and will start at 12.30pm (with registration from 12.00 noon) and conclude at 1.30pm.

# UNDERSTAND PENSIONS REGULATION & COMPLIANC



**If you're a compliance officer with a responsibility for pensions compliance, as well as considering the requirements of the Central Bank when preparing your annual compliance plan and deciding on your monitoring activity, it will be important for you to be aware of the requirements of the Pensions Authority and Revenue law and practice, writes Brian Macdonald of the ACOI Pensions Working Group.**

## Pensions Authority

**The current key priorities that direct the supervisory approach of the Pensions Authority are as follows:**

- Misappropriation of pension assets or contributions.
- Lack of governance or maladministration impacting on benefits / failure to pay benefits due.
- Defined Benefit solvency.
- Failure to provide prescribed information to members.
- Failure by regulated entities to submit accurate and timely data to the Authority.

You need to ask yourself how your compliance plan is aligned with the key priorities.

## Misappropriation of pension assets or contributions

**Consider the following questions:**

1. If your firm is involved with the administration of pensions, what procedures and controls are in place to ensure pension contributions are received from the employer/ trustees within 21 days of the end of the month in which the deductions were made from the employees' salaries or became due?
2. Have all monies received been subsequently invested (again within the prescribed time limits), can you evidence this?
3. Separately, have you validated the procedures recently to ensure they are adequate and what monitoring do you do to ensure the controls are working?
4. Where a breach is identified what are your "whistleblowing" procedures and are they effective? How many "whistleblowing" reports under Section 83 of the Pensions Act, 1990 (as amended) have you made so far this year to the Pensions Authority? If none, is that reasonable?
5. If you are a trustee, for the schemes you act as trustee are you aware of the employers who are serial late payers and what actions are you taking to address the issue?

# DING

# CE

*"Where a scheme does not meet the required funding standard then the trustees must arrange for a "funding proposal" to be prepared by an actuary setting out the recovery plan for the scheme and submit it to the Pensions Authority."*

## Lack of governance or malad-ministration impacting on benefits / failure to pay benefits due

Clearly where someone has been building up a pension pot during their working life then it is a key priority of the Pensions Authority to ensure that the benefits are both calculated correctly and paid on time to the correct person. The events that may result in the payment of benefits are on leaving employment, retirement or death. It is therefore important that both pension administrators and trustees have the appropriate procedures and controls in place to allow for this.

**Again, the following questions spring to mind;**

1. How does your firm identify when benefits become due and how and when are customers informed, what oversight do you have of this?
2. Are compliance checks in place across the business to validate the calculation of benefits? How do you ensure you are paying the benefits to the correct person?
3. When it comes to death benefits, how do you ensure that the correct benefits are insured and paid in accordance with the scheme rules? For example, are different benefits payable on the death of a member depending on their marital status?
4. How do you ensure that this information is kept up to date and accurate by all relevant parties so that the correct benefits are insured?

## Defined benefit solvency

Under the terms of the Pensions Act, 1990 (as amended) every Defined Benefit occupational pension scheme must produce an Actuarial Funding Certificate (every 3 years) and submit this to the Pensions Authority which certifies the solvency of the scheme i.e. the ability of the scheme's assets to meet its liabilities. How can you demonstrate that this has been done? Where a scheme does not meet the required funding standard then the trustees must arrange for a "funding

*"The trustees have responsibility for the ongoing management of the scheme and must invest the contributions and provide for the necessary assets to meet the benefits in line with the rules of the scheme."*

proposal" to be prepared by an actuary setting out the recovery plan for the scheme and submit it to the Pensions Authority.

The trustees have responsibility for the ongoing management of the scheme and must invest the contributions and provide for the necessary assets to meet the benefits in line with the rules of the scheme. In doing so the trustees need to assess whether the contributions continue to be adequate to provide the benefits under the scheme, both the current and future benefits. They should regularly discuss the funding position with the employer and seek additional contributions to the scheme as required.

The whole area of Defined Benefit scheme solvency is often in the news so I would encourage you to regularly check the Pensions Authority's website for any recent developments. Indeed, at the time of writing, the General Scheme of Social Welfare and Pensions Bill 2017 has just been published and proposes a number of changes in relation to Defined Benefit pensions. Access the link below and refer to "Part 3: Amendments to Pensions Act 1990":
*https://www.welfare.ie/en/downloads/GeneralSchemeSocialWelfarePensionsBills2017.pdf*

The importance of having early warning processes in place assists in the management of death benefits (see point 2 above) and Defined Benefit solvency concerns.

## Failure to provide prescribed information to members

**If your firm acts as a Registered Administrator (RA) for pension schemes then you should be aware of the core administration functions carried out by the RA for the trustees:**

- The preparation of the Annual Report and annual member benefit statements for each scheme,
- The maintenance of sufficient records to provide such services, and
- The submission of Annual Scheme Information (ASI) to the Pensions Authority

As well as ensuring the content of the Annual Report and member benefit statements comply with the

Disclosure of Information Regulations of the Pensions Act you also need to monitor that the documents are issued to the trustees within the prescribed timeframes. Is it part of your monitoring activity to check the documents are issued on time and that you report any breaches to the Pensions Authority? Even though not specifically called out as part of the RA core functions, the Pensions Act also requires information to be disclosed on the establishment of a scheme, when a member leaves employment, retires or dies, and on the winding up of a pension scheme. At each stage certain information must be disclosed and within a certain timeframe. It is therefore important that you are aware of the requirements in this regard and that you have the appropriate checks and controls in place to ensure compliance.

The Disclosure of Information Regulations is simply one part of the Pensions Act, 1990 (as amended) so it is important to be aware of all the provisions as the Act regulates Occupational Pension Schemes and Personal Retirement Savings Accounts (PRSAs).

As the RA has your firm correctly registered with the Pensions Authority and is there a procedure in place to renew the registration on an annual basis within the prescribed timeframe? Does it work?

## Failure by regulated entities to submit accurate and timely data to the Authority

Lastly, the Pensions Authority has made it clear to pension providers of the need to maintain and submit accurate data to the Authority in relation to the pension schemes they administer. It would be best practice therefore to carry out regular checks to make sure the data held on the Pension Data Register (PDR) of the Pensions Authority matches the data held by the RA and trustees. In addition, the ASI return made by the RA should align with the data in the Annual Report.

## Revenue law and practice

The legislation governing the tax treatment of pensions is contained in Part 30, Taxes Consolidation Act 1997. The Act grants discretionary powers to Revenue in relation to the approval of occupational pension schemes, personal retirement bonds (buy-out bonds), personal pension contracts and PRSAs. You should also be aware of the Revenue Pensions Manual which gives guidance on how the powers within the Act are exercised.

**Any compliance monitoring activity therefore needs to be conscious of the Revenue requirements and I would suggest at a minimum should cover:**

- Ensuring individuals taking out pension arrangements are eligible to do so.
- The contributions received by the pension arrangement do not exceed Revenue maximum funding limits.
- Refunds of contributions from a pension arrangement are made in line with Revenue rules.
- The payment of retirement and death benefits do not exceed Revenue maximum limits.
- Transfer payments received from or made to other pension arrangements are in line with Revenue requirements.
- Checks on the operation of Pension Adjustment Orders (PAO) when made against a pension arrangement. For example, on receipt of a PAO a number of checks should occur such as checking the legislative references, that the member details and scheme details are referenced correctly in the PAO, the type of PAO issued and so on to ensure the validity of the PAO. In terms of the operation of the pension arrangement where a PAO has been granted against it, compliance checks should monitor the transfer of pension benefits, the calculation of maximum benefits, the taxation of the retirement lump sum and the interaction with the limit on tax relieved pension funds.
- Deduction and remittance of tax as required under Revenue rules as well as the operation of Approved Retirement Fund (ARF) deemed distribution.

As you can appreciate there is clearly a lot to consider when implementing a compliance plan and running an effective monitoring programme in the pensions space. Clearly the requirements of the Pensions Authority and Revenue law and practice must be at the forefront of this.

As with all areas of compliance it is vitally important that you clearly document and record all steps you take so you are able to evidence compliance with the relevant requirements and obligations. If it's not formally documented – it didn't happen!!

***Brian Macdonald is Life & Pensions Technical Support Manager, New Ireland Assurance & member of the ACOI Pensions Working Group.*** ICQ

# OUTSOURCING: Recent Perspectives

**In a period of heightened regulatory interest as evidenced by the Central Bank of Ireland's (Central Bank) recent pronouncements in enforcement cases, thematic reviews and speeches to industry on outsourcing and corporate governance, Edwina Malaniff a member of the ACOI's Prudential, Regulation and Governance (PR&G) Working Group outlines some of the important outsourcing requirements for compliance professionals.**

"Is this outsourcing?" "Is it material outsourcing?" These two questions were put to attendees at the "Outsourcing – Recent Perspectives" seminar held on 23rd February 2017, organised by the ACOI Prudential and Governance Working Group. The speakers, Rob Cain, Arthur Cox and Chris Gallagher, Capita Asset Services, in posing these questions, engaged attendees and highlighted to all the debate that can ensue when considering such matters.

## Fundamental Expectations

As highlighted at this seminar, it would appear that the fundamental expectations of the Central Bank in respect of outsourcing matters include:

- That the Board and senior management retain ultimate responsibility for outsourced activities;
- That any outsourcing arrangement requires strong governance and proper oversight (with challenge from the Board / senior management);
- That there is appropriate risk management including robust requirements for the receipt of relevant risk information;
- Compliance with European Banking Authority (EBA) guidelines – which reflect market practice across the EU since 2006;
- And importantly – that the above apply to intra-group outsourcings as well.

The guidance emanating from the Central Bank echoes a number of principles found in the EBA (formerly CEBS) "Guidelines on Outsourcing 2006" ***(1)***. These guidelines are a rich resource of basic outsourcing principles as well as more granular requirements. Granular matters include content to be provided in a firm's outsourcing policy ***(2)*** as well as certain provisions to be incorporated in a written agreement between the firm and the outsourced service provider.

The Guidelines also offer helpful guidance for a firm to apply when considering if their delegated arrangements would be considered "material activities".

Activities considered to be material are:

- Activities of such importance that any weakness/ failure could have a significant effect on the firm's ability to meet its regulatory responsibilities and/or to continue in business;
- Any activities requiring a licence;
- Activities that have a significant impact on risk management;

Importantly, compliance professionals must be aware that those outsourced activities amounting to "material activities" require notification to the Central Bank.

## Outsourcing Oversight

In respect of the oversight of outsourcing arrangements, the Central Bank's expectations around mitigating and managing outsourcing risks are set out in their response to the recent thematic review by their Investment Firms and Funds Supervision Department ("IFSS") ***(3)***. It is here a Compliance professional may gain some insight into the Central Bank's expectations on monitoring and reporting on outsourced activities.

The Central Bank recommends that firms consider the following:

- **Monitoring** – that key performance indicators and monitoring tools are embedded in the outsourcing risk framework;
- **Reporting** – that it be sufficiently detailed and frequent;
- **Appraisal** – rigorous initial due diligence and ongoing appraisals of service providers;
- **Business continuity** – succession/ remedial action plans (with robust testing);
- **Outsourcing policy** – taking into account the entire life cycle of the outsourcing arrangement;

The speakers referred to the harmonised set of outsourcing rules /guidance provided in the UK by the Financial Conduct Authority. In Ireland there are a number of sources to which a Compliance professional must reference when striving for outsourcing compliance. Notwithstanding that these sources may represent guidance for particular financial services industry sectors, the underlying principles can be applied to other financial service entities and should therefore be considered by all Compliance professionals.

***Edwina Malaniff, Compliance Manager, State Street Global Advisors Ireland Limited and member of the Prudential, Regulation & Governance Working Group.*** ICQ

**In the Autumn 2017 edition the ACOI Funds Working Group will consider the extensive use of outsourcing and the obligations it imposes within the funds sector.**

*(1) https://www.eba.europa.eu/documents/10180/104404/GL02OutsourcingGuidelines.pdf*
*(2) https://www.eba.europa.eu/documents/10180/103861/EBA-BS-2011-116-final-EBA-Guidelines-on-Internal-Governance-%282%29_1.pdf*
*(3) https://www.centralbank.ie/docs/default-source/Regulation/how-we-regulate/supervision/thematic-review/gns-4-1-2-3-outsourcing-arrangements.pdf?sfvrsn=2*

# Lifelong Learning throu

**By accepting the invitation to take up an ACOI designation a member embraces the ethos of life-long learning by keeping abreast of developments in the dynamic field of regulatory compliance and ethics. It is a statement that they have attained a level of technical competence, writes Finbarr Murphy, Director of Education and Professional Development, ACOI.**

As members of the ACOI you may be considering to study, or know of someone that would like to study, compliance. Performing due diligence is a crucial step in your job and it should also be crucial in selecting what you will study. The ACOI provide the most comprehensive range of regulatory compliance designations underpinned by university accredited programmes in Ireland. The designations offered will support you at all stages in your career from providing essential core knowledge to advanced and specialist knowledge.

I urge you to visit our website: **www.acoi.ie/education/** to review the various offerings. In semester 1 of the 2017/18 academic year applications from interested and eligible members are being sought to complete programmes leading to the following designations;

## Licentiate of the Compliance Officers in Ireland (LCOI)

| Associated Programme / Entry Route | Award | Programme Details |
|---|---|---|
| Professional Diploma in Compliance | UCD, NFQ Level 7 | 4 modules, each 5 ECTs, 40% pass mark, delivered by distance learning over one semester (12 weeks). The primary learning resource is a comprehensive4 modules, each 5 ECTs, 40% pass mark, delivered by distance learning over one semester (12 weeks). The primary learning resource is a comprehensive manual supplemented by online webinars, learning planner and sample questions. |

The LCOI designation and the Professional Diploma in Compliance are considered as the compliance practitioners' benchmark designation and qualification respectively. The Professional Diploma in Compliance is the only university accredited qualification in compliance. It remains extremely popular with students entering the compliance space, practitioners refreshing their knowledge and/or seeking a formal qualification in the disciple.

## Fellow of the Compliance Officers in Ireland (FCOI - MSc)

| Associated Programme / Entry Route | Award | Programme Details |
|---|---|---|
| MSc in Compliance | UCD, NFQ Level 9 | 7 modules and an Applied Project, each module is 10 ECTs and the Applied Project is 20 ECTs, 90 ECTs. 40% pass mark, taught programme, 5 full-Saturdays for each module. Two semesters per year, two modules offered in each semester (12 weeks). |

## Fellow of the Compliance Officers in Ireland (FCOI - MA)

| Associated Programme / Entry Route | Award | Programme Details |
|---|---|---|
| MA in Ethics (Corporate | DCU, NFQ Level 9 | 6 modules and a Thesis, each module is 10 ECTs and the Thesis is 30 ECTs, 90 ECTs. 40% pass mark, taught programme, one weekday evening. Two semesters per year. |

# ugh ACOI Designations

The FCOI designation is the highest designation the ACOI offers. Holders of this designation will be the future leaders in control functions and advisers in financial services

## Certified Data Protection Officer (CDPO)

It will take time to prepare for the introduction of the General Data Protection Regulation (GDPR), the new EU data protection framework. It contains many additional obligations effective from 25th May 2018. One such obligation is that in certain circumstances data controllers and processors must designate a Data Protection Officer (the DPO) as part of their accountability programme. The DPO will need sufficient expert knowledge. One of the best ways to acquire knowledge in a fast and efficient manner is to educate your-self. This is recognised by the Data Protection Commissioner, Helen Dixon;

*"The Irish DPC welcomes ACOI's recent increase in the offering of its data protection certification programme to twice a year. Staff with skills necessary to support organisations in lawfully collecting and safeguarding personal data are in growing demand as we enter into the final un-up to the General Data Protection Regulation implementation date in May 2018. We wish all students on the programme every success."*

Topics on this programme range from the regulations, the impact of the cloud, social network, rights of privacy and treatment of data.

| Associated Programme / Entry Route | Award | Programme Details |
|---|---|---|
| Professional Certificate in Data Protection | UCD, NFQ Level 9 | 1 module, 10 ECTs, 40% pass mark, taught programme, 5 full-Saturdays in one semester. |

## Programmes of Strategic Importance attracting government funding

Both the MSc in Compliance and Professional Certificate in Data Protection attract Summit Finuas Network funding, www.summitfinuasnetwork.ie. This is recognition of the strategic importance placed on the content of each programme. Funding is available for a limited number of places on a first come first served basis.

## Sectorial specific programmes that the ACOI endorse and members study on are:

| Programme | Sector | Award |
|---|---|---|
| Professional Certificate in Conduct Risk, Culture & Operational Risk Management | Banking | UCD, NFQ Level 8 |
| Professional Certificate in Investment Fund Services Risk Management (Operational Risk, Conduct Risk and Risk Culture) | Funds / Investment Management | UCD, NFQ Level 8 |

### In the case of both programmes;

**Structure:** 2 modules, 10 + 5 ECTs, 40% pass mark, delivered by blended learning (webinars + workshops) over one semester (12 weeks).
**Content:** Operational Risk Management Practices, Risk Management Frameworks, Culture and Conduct Risk.
**Recognition:** In addition to receiving an award from UCD the student will receive the PRMIA Operational Risk Manager award. The Professional Risk Managers International Association is the globally recognised leader in risk management education.

### Cross-disciplinary and non-sector specific programme – open to ACOI members

The ACOI and Chartered Accountants Ireland collaborated to offer its members the Diploma in Risk Management, Internal Audit & Compliance. This is a 6 module programme that can be completed over 6 months. The programme is aimed at those who work or aspire to work in a professional capacity in risk or internal audit or compliance roles. The course will equip you with an understanding of how to build, effectively communicate and influence on risk management, internal audit, governance and regulatory compliance operations. The course is available by classroom and distance learning.

### Lifelong learning – keeping your knowledge current

There has been a significant increase in members taking one of our educational programmes and we thank you for the support and welcome your feedback. Attendance at CPD and other events now regularly exceeds 200 people. ACOI continues to engage with the Central Bank and other regulators to support members. Many members continue welcome our invitation to take-up our designations. This bodes well for the future, creating a vibrant compliance community by you the members, acknowledging the role the ACOI has to play and your own responsibility in the continued professionalization of the compliance field. This is based on the shared belief that by accepting the ACOI invitation to take up a designation you will maintain the knowledge acquired through your studies. Knowledge and education are the foundation and bedrock of any profession.

***Finbarr Murphy, Director of Education & Professional Development, ACOI.*** ICQ

***If you should have any queries on any programme the ACOI offers please do not hesitate to contact me at finbarr.murphy@acoi.ie or 01-779 0202.***

## EVENT SCHEDULE FOR JULY & AUGUST 2017

| Date | Event | Venue | Time | Indicative CPD |
|---|---|---|---|---|
| **04.07.17** | New Data Protection Requirements for Credit Union | TBC | 12.30 – 1.30 pm Seminar | 1 |
| **12.07.17** | Train-the Trainer | Hilton Charlemont | 9.00 – 11.00 am Workshop | n/a |
| **22.07.17** | PDC Exam Preparation Session | UCD Belfield | 10.00 – 1.00 pm | n/a |
| **10.08.17** | Building Blocks 4/6 – Planning & Monitoring | Hilton Charlemont | 9.00 – 11.00 am Workshop | 3 |
| **16.08.17** | Program Opening Evening | Institute of Banking | 4.00 – 7.00 pm | n/a |
| **29.08.17** | Data Protection Update from the ODPC | Chartered Accountant House | 12.30 – 1.30 pm Seminar | 1 |

OVERVIEW
Governance

# OVERVIEW of Membership of ACOI Working Groups

## Membership of the AML Working Group

| | |
|---|---|
| 1 | Kathy Jacobs - Chair |
| 2 | Pamela Doyle |
| 3 | Tara Gordon |
| 4 | John Higgins |
| 5 | Stephen Hudson |
| 6 | Brian Kavanagh |
| 7 | Mairead Kirwan |
| 8 | Kevin Loughnane |
| 9 | Amanda Lucas |
| 10 | Shane Martin |
| 11 | Jackie Murphy |
| 12 | Cormac ó Braonáin |
| 13 | Denise Whelan |

## Membership of the Consumer Protection Working Group

| | |
|---|---|
| 1 | Gerard O'Connell - Chair |
| 2 | Deirdre Haverty - Vice Chair |
| 3 | Frances Bleahene |
| 4 | Fiona Bourke |
| 5 | Susan Clerkin |
| 6 | Mary Dooley |
| 7 | Denise Dunne |
| 8 | David Madigan |
| 9 | Eoin O'Connor |
| 10 | Ciara Rigney |
| 11 | Christina Toher |

## Membership of the Credit Union Working Group

| | |
|---|---|
| 1 | Ellen Farrell - Chair |
| 2 | Sharon Farrell - Vice Chair |
| 3 | Mick Casey |
| 4 | Christopher Fitzpatrick |
| 5 | Brendan Kelly |
| 6 | Fiona Lawlor |
| 7 | Mairead MacQuaile |
| 8 | Shane Martin |
| 9 | Lynn McDaid |

## Membership of the DP & Tech Working Group

| | |
|---|---|
| 1 | Aisling Clarke - Chair |
| 2 | Samantha Fletcher-Watts - Vice Chair |
| 3 | Rory Byrne |
| 4 | Emma Cramp |
| 5 | Mary Colhoun |
| 6 | Rob Corbet |
| 7 | Oliver Irwin |
| 8 | Cathryn Kendal |
| 9 | Ian Long |
| 10 | John Magee |
| 11 | Tom O'Connor |
| 12 | Daniel Patterson |

## Membership of the Funds Working Group

| | |
|---|---|
| 1 | Keith Rothwell - Chair |
| 2 | Brian Cahalin - Vice Chair |
| 3 | Ken Sharkey |
| 4 | Valerie Bowens |
| 5 | Eva Breslin |
| 6 | Lisa Cotter |
| 7 | Antoinette Drinkwater |
| 8 | Riona Dunne |

## Membership of the Funds Working Group (cont.)

| | |
|---|---|
| 9 | Carina Myles |
| 10 | Antonella Narducci |
| 11 | Conor O'Donnell |
| 12 | Ciara O'Sullivan |
| 13 | Colin Reynolds |
| 14 | Aidan Rogers |
| 15 | Bernard Williams |

## Membership of the Pensions Working Group

| | |
|---|---|
| 1 | Brendan McWeeney - Chair |
| 2 | Brian MacDonald - Vice Chair |
| 3 | Lorraine Conlon |
| 4 | Joseph Doherty |
| 5 | Fiona Morahan |
| 6 | Gemma Herrity |

## Membership of the PR&G Working Group

| | |
|---|---|
| 1 | Rose Marie Kennedy - Chair |
| 2 | Robert Cain - Vice Chair |
| 3 | Tom Crowley |
| 4 | Lynda Kenny |
| 5 | John Kernan |
| 6 | Edwina Malaniff |
| 7 | Conor Molloy |
| 8 | Niamh O'Mahoney |
| 9 | Sarah Dineen |
| 10 | Elaine Staveley |
| 11 | Miriam Waldron |

# THE ATTRIBUTES OF THE Effective Compliance Officer

**The history of financial crises in recent years has led to an increase in regulations, laws and strengthening of internal controls within an organisation. There has also been an increase in penalties imposed by regulators - both financial fines, sanctions and reputational damage – and failure to comply can be very costly. All these have the effect of changing the role and functions of the modern-day compliance officer.**

**The Niall Gallagher Professional Diploma in Compliance Scholarship'** was launched to promote the importance of further education and recognition of professional certification in the advancement of an individual in their career in compliance. It is named the 'Niall Gallagher Professional Diploma in Compliance Scholarship' in recognition of Niall's contribution to the field of Ethics and Compliance and in particular for his pivotal involvement in the formation and development of the ACOI. In the Spring 2017 edition of ICQ, the essay from the inaugural winner, Ms Anna Mulhall was featured. In a continuation of the series, the second placed essay from Rosemary Atuokwu is now reproduced. Rosemarys' prize was ACOI membership for two years.

Historically, the compliance officers' role was once a functionary, middle-management job who had no significant influence and authority within an organisation. But today, with regulations such as Sarbanes-Oxley, the compliance officer has been given the responsibility of managing compliance issues within an organisation, maintaining records of what organisation can and cannot do, transparency and accountability to the board.

The compliance officer in addition to corporate compliance should also take ownership of the organisation's ethical issues. The compliance function has an advisory and oversight role with the various business areas within the organisation. In most big organisations, the compliance function provides a second line of defense by testing and reviewing controls and by providing independent verification to senior management that these controls are working. To discharge these responsibilities the compliance officer should either be a member of senior management of the firm or have direct reporting line to senior management.

According to Fitness and Probity standards, the compliance officers' role is a Controlled Function (CF), because he/she is involved in ensuring, controlling or monitoring compliance with an institutions' obligations. This role will vary depending on the size, management and control arrangements within an organisation and the extent to which the activities of the organisation are regulated.

**As a result of the above, a compliance officer to be effective in their role, must possess the following attributes;**

## Resourcefulness

To be effective in their role, a compliance officer must be resourceful and have the right professional training. The regulatory environment within all industries (both financial and non-financial) are complex and constantly changing. A good compliance officer must have the ability to interpret complex issues and stay on top of new regulations (upstream regulations), ensuring the organisation is adequately resourced to meet these requirements. He/she needs to understand the company's operations, strategies, key players, culture and competitive environment to advise and raise concerns where necessary.

## Focused, diligent and organised

An effective compliance officer must be focused and diligent. He/she must ensure they have a clearly defined structure, responsibilities and job description. To avoid conflicts of interests, he/she must remain focused on monitoring and promoting a sound compliance program. The compliance program must be organised and well documented. All employee training must be completed within an agreed timeframe and certifications of completion must be kept on file. All internal audits of control processes and investigations must be thoroughly conducted and records of breaches and remedial actions undertaken must be maintained.

## Independent and firm

An effective compliance officer must protect the best interest of the organisation. Sometimes the decisions and recommendations of the compliance officer might be contrary to the interest of top-level management or the board of directors. Therefore, the compliance officer must possess the ability and strength of character to make sound decisions and have the "backbone" to stand by those decisions. He/she must have authority and possess a senior role to take and implement the necessary actions. Regulators have held individuals responsible for non-compliance. For example, the Financial Industry Regulatory Authority (FINRA) fined Raymond James & Associates' anti-money laundering compliance officer, Linda L. Busby $25,000 and received a three-month suspension from association with any FINRA member firm.

## Communication and people skills

A compliance officer must possess strong communication skills. He/she must be able to express clearly decisions to all stakeholders involved. The compliance officer must be able to interpret corporate and local regulatory requirements as they affect products and services that are undertaken by the organisation. An effective compliance officer must be able to engage in constructive dialogue when conflicting interests are at play. The compliance officer must create an environment where employees feel comfortable to discuss issues and file complaints.

## Responsive and proactive

An effective compliance officer must be responsive and proactive in dealing with complaints when they arise. They should not wait for problems to arise but endeavour to make compliance part of everyday business within the organisation. He/she must respond immediately to concerns, allegations and to protect internal whistle-blowers. The compliance officer must assess potential risks and work with management in developing concrete and effective policies and measures to mitigate these risks. Compliance programs must be active and dynamic in line with developments and trends. There must be regular compliance training for staff to inform them of their obligations to comply with local and international laws/regulations and the consequences of non-compliance or violations of these laws.

## Cooperative and professional

An effective compliance officer must be cooperative when asked to present/report findings of internal investigations by management, auditors or law enforcement agencies. The compliance officer must be able to present findings in a professional manner and be cooperative with law enforcement authorities during investigations.

## Ethical and principled

An effective compliance officer must be ethical, principled and fair. He/she must objectively access all facts and circumstances of an allegations before reaching a conclusion. He/she must be fair when gathering supporting documentation, when interviewing staff involved and in enforcing discipline.

**In Conclusion**

For the compliance officer to be effective, he/she must have the necessary level of influence and authority within the organisation and be adequately resourced to carry out their responsibilities. They must have independent reporting lines to the board and senior management. The compliance officer must align the compliance program with the company's overall strategy to encourage a business that is responsibly conducted and ethical in behaviour. The compliance officer should aim to create a compliance program that is based on the organisation's values, as one incident can put a company's reputation at risk and potentially its ultimate existence. This will require the compliance officer to be able to influence staff and management that by being compliant, risk can be reduced and business opportunities increased.

***Rosemary Atuokwu is a Senior Fund Accountant with BNP Paribas Securities Services.*** ICQ

# EVENTS 2017

**1 09.05.17 Privacy Impact Assessments (PIAs) Workshop** L-R: Mary Colhoun, Eir; Aisling Clarke, ACOI Council Member & Event Chair and Anne-Marie Bohan, Matheson.

**2 27.04.17 Financial Sanctions in the Funds Sector & EMIR Update** L-R: Brian Cahalin, Appian Asset Management & Funds WG; Niamh Lynn, Central Bank of Ireland and Conor O'Donnell, The Citco Group of Companies.

**3 04.04.17 Lunchtime with the Ombudsman** L-R: Ger Deering, Pensions & Financial Services Ombudsman; Gemma Roche, Willis Towers Watson & Event Chair and Brendan McWeeney, Harvest Financial Services Ltd & Chair of Pensions WG.

**4 21.03.17 Building Blocks for Effective Compliance – Risk Assessment** L-R: Tom O'Connor, HedgeServ and Anna Mulhall, KPMG.

**5 28.03.17 MiFID II – Are you ready?** L-R: Aoife McGee, Anna Murphy, Central Bank of Ireland; Gerry O'Connell, Chair of Consumer Protection WG & Event Chair and Denise Murphy, Central Bank of Ireland.

**6 24.05.17 AML Cultural Diagnostic Tool Seminar / How's your AML Culture?** L-R: Mairead Kirwan, permanent tsb; Finbarr Murphy, ACOI Executive and Tara Casserly, UCC & Durrus Compliance Diagnostics.

**7 25.05.17 Building Blocks for Effective Compliance – Culture & Conduct** L- R: Chris Martin and Ciaran Walker, Eversheds Sutherland; Eavan Garvey, Bank of Ireland and Tim Dyball, Goodbody Stockbrokers. ICQ







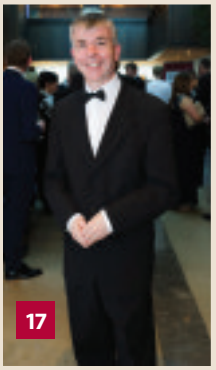
# ACOI Annual Dinner 2017









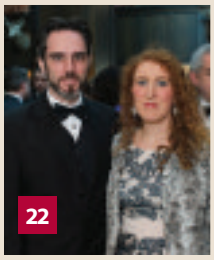



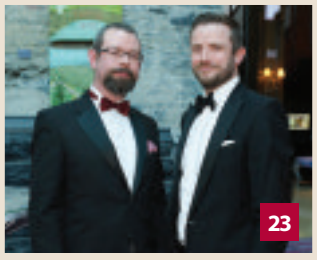


**19.04.17 ACOI Annual Dinner**

**8** Simon Treanor, Allison Coughlan, Christophe Rey. **9** Philip Brennan, ACOI Fellow. **10** Sean Sweeney and Ciarán O'Connell, Paragon Recruitment. **11** Olivia Dunning, Rabobank, Aisling Clarke, ACOI Council Member. **12** Rory Gallagher, Stephen Hudson, Albert Keirse, New Ireland Assurance. **13** Kathy Williams, IPB Insurance & Jennifer Coogan, AIB Bank. **14** Linda Valentine, VHI. **15** Olivia Dunning, Rabobank, Evelyn Cregan, ACOI Chief Executive, Declan McHugh, Goodbody Fund Management. **16** Lynda Elliott and Anna Mulhall, KPMG. **17** Kevin Byrne. **18** Niall Gallagher, ACOI Fellow, Pat Liddy, Historian, Séamus Canning, ACOI Council Member.





**19.04.17 ACOI Annual Dinner (Continued)**

19 Niall Gallagher and Sean Wade, ACOI Fellows and VHI Team. 20 Jean Heylin and Estelle Davis, Brightwater Recruitment Specialists. 21 Slyvia Cronin, Central Bank of Ireland; Michael Feeney, Institute of Banking & Kathy Jacobs, ACOI Council Member. 22 Gareth Walsh, Sum Up and Sinead Walsh, Bank of Ireland. 23 Terry McPartland, Grant Thornton and Peter Mansfield, AON. 24 VHI Team. 25 Dermot Naughton, Mainstreet International Finance. 26 Dr Diarmuid Bradley, Institute of Banking, Clive Kelly ACOI President, Dr Paul Quigley, Institute of Banking. 27 Bryan O'Reilly, City Learning. 28 Caroline Hollick-Ward, ACOI Executive, Terry McPartland, Grant Thornton, Peter Mansfield, AON and Coleman Hudson ACOI Council Member. 29 Dolores Geaney, Investec; Thomas Gilligan and Nancy Egan Investec. 30 Anne Marie McKiernan, Central Bank of Ireland. 31 Aine Hickey, Intertrust Ireland. 32 Coleman Hudson and Mary Noonan, ACOI Council Members; Oliver Jordan, BOI; Melanie Blake, ACOI Council Member; Olivia Dunning, Rabobank and Seamus Canning, ACOI Council Member. 33 Finbarr Murphy, ACOI Executive; Sinead Ovedon, PwC; Jason Palmer, ACOI Council Member and Julie Winder, PwC. 34 Broadgate Search. 35 Becky Bristow, Chartered Accountants Ireland. 36 Fiona Coloe, Kathy Williams and Sonia Wielinska, all IPB Insurance. 37 Cormac O'Neill and Mary Ann English, both City Learning. 38 Bill Hannan, ACOI Fellow. ICQ

















**CHARITY MONEY RAISED AT ACOI ANNUAL DINNER 2017:** 39 and 40 Evelyn Cregan, ACOI Chief Executive and Clive Kelly, ACOI President ICQ

# Banking

## Domestic

**09 MAY 2017**

The Central Bank's "Thematic Inspection of Regulatory Reporting by International Banks" is published.

**05 APRIL 2017**

The Credit Guarantee Scheme 2017 is published.

## European

**09 MAY 2017**

European Central Bank Annual Report 2016 is published; European Central Bank publishes Guidelines and Recommendations specifying common specifications for the exercise of discretions available in relation to less significant institutions.

**05 APRIL 2017**

European Banking Authority publishes LCR Guidelines; European Banking Authority publishes Regulatory Technical Standards on the disclosure of encumbered and unencumbered assets; European Central Bank publishes guidance to banks on non-performing loans.

# Funds

## Domestic

**09 MAY 2017**

Irish Funds have revised Guidance Paper 6.

**05 APRIL 2017** - Central Bank publishes the latest version of the AIF Rulebook dated March 2017; Central Bank publishes updated UCITS Q&A

## European

**09 MAY 2017**

ESMA updated Q&As on the application of the AIFMD Directive and the UCITS Directive; European Parliament adopts the Money Market Funds Regulation.

**05 APRIL 2017**

Economic and Monetary Affairs Committee of the European Parliament adopts a draft report on the proposal to amend the EuVECA Regulation and EuSEF Regulation; Commission adopts delegated regulation on key information document for PRIIPs.

# Insurance

## Domestic

**09 MAY 2017**

Department of Finance consults on Insurance Distribution Directive; Insurance Ireland publish Annual Report 2016.

**05 APRIL 2017**

Central Bank publishes consultation paper on industry funding levies; Central Bank publishes Insurance Quarterly newsletter.

## European

**09 MAY 2017**

EIOPA publishes Thematic Review of consumer protection issues in the unit-linked market; European Commission proposals on the EU and US bilateral agreement on (re) insurance.

**05 APRIL 2017**

Commission adopts a Delegated Regulation supplementing the Regulation on key information documents for packaged retail and insurance-based investment products; Commission adopts a Regulation on the calculation of technical provisions and basic own funds for the purpose of Solvency II reporting.

# Investment Firms

## Domestic

**09 MAY 2017**

Director of Asset Management Supervision in the Central Bank address MiFID II.

**05 APRIL 2017**

Investment Firms Regulations 2017 are published; Central Bank publishes guidance and Q&As on the Investment Firms Regulations 2017; Central Bank launches a Consultation on the protection of retail investors in relation to the distribution of Contracts for Difference.

## European

**09 MAY 2017**

ESMA publishes final technical advice to the European Commission regarding supervisory fees for Trade Repositories under the Securities Financing Transactions Regulation; ESMA publishes

update to Q&As regarding the European Markets Infrastructure Regulation and validation rules; ESMA publishes several Q&As in relation to the Markets in Financial Instruments Directive II.

**05 APRIL 2017**

ESMA publishes Q&As on the Central Securities Depositories; ESMA publishes regulatory technical standards on package orders for which there is a liquid market.

# Cross Sectoral

## Domestic

**09 MAY 2017**

Central Bank announces published its 2016 Annual Report and its 2016 Annual Performance Statement; Department of Finance launches Consultation on Crowdfunding.

**05 APRIL 2017**

On the Domestic Front: Financial Services Ombudsman Council 2017 Levies and Fees are published; Central Bank introduces new Consumer Protection Risk Assessment (CPRA) Model; Central Bank launches Consultation on New Methodology to Calculate Funding Levies.

## European

**09 MAY 2017**

National application of the Fourth Anti Money Laundering Directive is triggered; ESMA publishes opinion on Market Abuse Regulation accepted market practices in relation to liquidity contracts.

**05 APRIL 2017**

7 Delegated / Implementing Regulations supplementing the Central Securities Depositories Regulation are published; European Commission publishes Shareholders' rights directive Q&A; Commission launches Consultation on the operation of the European Supervisory Authorities. ICQ

# MEMBER Profile

## Margaret Colgan

**Margaret Colgan, Senior Consultant, Complaints Handling in Ulster Bank and member of the ACOI Consumer Protection (CP) Working Group**

***What did you want to do when you left school?***
Following the Leaving Cert like most people in those days I was unsure of what I wanted to do so I attended what we called 'Commercial College' and proceeded with my Pitman exams. Through this I got my first 'real job' in EBS where I stayed for 15 years until other ventures beckoned.

***How did you enter into the world of compliance?***
In 2006 I had oversight of the compliance function for Mason Financial Services where I had at last found my niche! It helped that my MD encouraged compliance and supported me in this regard. While I was looking for other compliance allies or associates I came upon the ACOI by chance which was relatively new at the time. I then found out about the compliance exams and completed my PDC in 2008-2009.
I subsequently joined the ACOI CP Working Group at an exciting time of evolving compliance requirements. The CP working group also covered Minimum Competency under its remit which was a challenging subject at the time.

***What do you consider are the challenges ahead for your industry?***
Now there's a question! Working in the midst of constant evolution poses challenges in itself. However, this can be managed by maintaining and sharing up to date knowledge, maintain ongoing monitoring of existing controls for effectiveness, be aware of upstream regulation and have a clear strategy for effective implementation of same. I would say maintain momentum and beware of complacency. With regard to current challenging topics I would mention Outsourcing, Product Governance & Oversight, Integrity and Conduct risk.

***How would you describe your management style?***
Using care, diligence and integrity in all that I do.

***What's the most valuable advice that you have been given?***
Trust your instinct.

***A professional and personal accomplishment you are proud of?***
Professionally, researching, analysing, interpreting and implementing CPC and MCR 2006 - solo! And getting it right first time! Also obtaining my PDC independently.

Personally, I stopped smoking 16 years ago. I am still proud (and very, very glad - despite the weight gain!).

***What are you currently watching and listening to?***
Watching any good murder mystery and listening to anything I can dance to - especially in the kitchen.

***What's your favourite book of all time and what book changed your life?***
I don't have a particular favourite, but any fiction I can lose myself in temporarily. The book that changed my life is Allen Carr's *Easyway to Stop Smoking*.

***How do you relax and unwind?***
Walking locally in Dollymount and the cliffs of Howth, Reading and maybe even a dance now and then!

***What's your favourite restaurant?***
Hemmingways, Clontarf

***Where is your favourite place in Ireland?***
Any of the beautiful beaches in north county Dublin and anywhere in West Cork or Kerry.

***An interesting fact about you?***
Many years ago I used to love flying small planes but it was too expensive at the time so I couldn't continue with lessons. I also did a couple of parachute jumps –solo – with no modern health & safety back up! ICQ

> *"Many years ago I used to love flying small planes but it was too expensive at the time so I couldn't continue with lessons."*

# Job Notifications – The Easy Way

**Are you aware that ACOI runs a Professional Compliance Register? What is it? and How do you opt in?**

The ACOI is periodically approached by employers requesting that we advertise open positions within the Compliance sector.

ACOI maintains a register of independent compliance professionals who have opted in to receive notifications, by email, when these vacancies become available. You could receive up to 4 notifications a month.

**The Pro's**

- This service is provided free of charge to ACOI members only.
- You receive live, active relevant job vacancies directly to your email address.
- It is a completely confidential service.

**How to register:**

- Application forms can be found online at www.acoi.ie

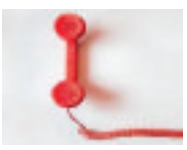
You will need to be logged in as a member, and the form is accessible through this link: Professional Compliance Register Application Form

Please download and complete the application form. Post the original signed form to ACOI, 5 Fitzwilliam Square, Dublin 2.

- Alternatively, phone ACOI Offices on 01 779 0200 and a form will be emailed directly to you.

**How to opt out:**

- Simply send an email to info@acoi.ie, requesting to be removed from the register.



**If you are an employer seeking to submit a vacancy:**
Please send your job specification, including appropriate contact details to info@acoi.ie


The Association of Compliance Officers in Ireland,
Lower Ground Floor,
5 Fitzwilliam Square,
Dublin 2,
Ireland.

For all membership and events enquiries,
please contact:
Phone: +353 - 1 - 779 0200
Email: info@acoi.ie

For all education-related queries,
please contact:
Phone: +353 - 1 - 779 0202
Email: finbarr.murphy@acoi.ie

www.acoi.ie