
ICQ
IRISH COMPLIANCE
QUARTERLY
Spring 2018
THE VOICE
Compliance Issues
and Topics
Building Blocks
Event Series
Data Protection
Bill 2018
COVER
STORY
IRELAND'S
FINTECH
OPPORTUNITY
AML Culture
So what
is corruption?
PLUS: PENSIONS REGULATION: TARGETED
REVIEW OF INTERNAL MODELS [TRIM]
ACOI

Contents

page 02
Contents

page 03
CEO Address:
Evelyn Cregan,
Chief Executive, ACOI

page 04
The Voice:
New Feature from ACOI President, Clive Kelly, to raise compliance issues and topics affecting ACOI Members

page 06
Cover Story
Richard Walsh,
Head of Digital & Payments, Banking & Payments Federation Ireland

page 12
Cloud Computing:
Considerations for Secure Adoption

page 16
Managing Financial Sanctions Risk:
Central Bank Guidance on Fund Administrator Outsourcing

page 18
Prudential Regulation & Governance:
Targeted Review of Internal Models [TRIM] – the inspection process

page 22
AML Update:
So what is corruption?

page 29
Events Update:
Building Blocks Series

page 30
DP & Tech:
Data Protection Bill 2018

page 34
Education:
Niall Gallagher Professional Diploma in Compliance Scholarship

page 37
IFCA:
When Failure Is Not An Option

page 44
News Tracker:
in Association with **A&L Goodbody**

page 46
Member Profile:
Brendan McWeeney,
Head of Compliance, Harvest Financial Services Limited

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.

CEO UPDATE

"We are very grateful for the support and time given by so many members across Committees and Working Groups of the Association"

Welcome to the Spring edition of the ICQ and let's hope that we have left the wintry conditions well behind us. In January we announced the winners of The Niall Gallagher Professional Diploma in Compliance Scholarship Award and we have the winning submission included in this publication. Well done to all those who entered. We will feature all winning entries throughout the year ahead.

Following our AGM held on 17th January, we have had a change in our Council, Ms Denise Whelan has retired from Council and we thank Denise for her contribution to the Association and we welcome the appointment of Mr. Fintan Byrne as a member of Council. All those contributing to the Association do so on a voluntary basis, we are very grateful for the support and time given by so many members across Committees and Working Groups of the Association, in particular, the contribution from our members of Council.

We continue to have strong interest in the academic programmes running in Semester 2 which started in February 2018. The Professional Certificate and Diploma in Compliance, PDC programmes leading to the LCOI, run three times a year. The two professional certificates, in Financial Crime Prevention and in Data Protection continue to attract very good numbers. Successful completion of these two certificates leads to an invitation to take up designations of Certified Financial Crime Prevention Practitioner and a Certified Data Protection Officers respectively. We will soon be launching an exciting new programme starting in September 2018, the Professional Certificate in Professional Certificate in Ethical Practice in Financial Services and, do note, the MA in Ethics – Corporate Responsibility programme is also available to members.

On the professional development front, the Building Blocks series is open for booking – the six events in the series are available to book. We know it continues to be a very busy time for compliance practitioners with MiFID 11 and PSD2 introduced in January, GDPR coming in May and 4AMLD expected soon. We continue to have CPD events to support you in your roles. We will have the Education & Careers evening in June; this is a great opportunity to hear from recruiters what is happening in the Compliance market and to hear from us and our educational partners of courses that are available for you and your colleagues for the next academic year.

We are delighted to announce a second Regional Chapter has been established in the South based in Cork following the launch of the first Regional Chapter in the South West, based in Limerick in quarter 4 of 2017. See more on our website on how to become involved in the chapters.

Ensuring that we are considering global issues, this publication shares an article from our Australian IFCA colleagues and shows us the similarity of issues met by our compliance colleagues around the world.

We are always looking for new members for Committees and Working Groups, so we encourage you to get involved in the Association. The Association is about you and for you, the members, so if there are things you would like to hear more about or things you would like to see us do more of, or differently, please get in touch with us and let us know.

We look forward to seeing you at our events soon. ICQ

Evelyn Cregan,
CEO

WELCOME to the SPRING 2018 Edition of ICQ

Dear Member,

You are very welcome to the Spring edition of our ICQ and our second "Voice of Compliance" feature.

This feature has been introduced for you, our members, to raise issues and concerns facing you as compliance officers and also to give you an opportunity to comment through your President on those issues and concerns.

We started this year with a fantastic event making sure you were "Fit for Fintech". We heard from Gerry Cross, Central Bank and Colm Heffernan, Fenergo on the potential for fintech and technology generally to provide solutions to assist organisations and compliance officers.

A point was made to Gerry on the ability of fintech/regtech solutions to assist in the broader aim of helping organisations improve their risk and compliance culture, one of the areas of focus for regulators.

The increasing ability of technology to assist in the more repetitive/ mundane (however necessary) tasks which compliance officers and their teams undertake frees up compliance officers and their teams to focus on the potentially greater value adding role of driving cultural change in their organisations. It was very positive to hear Gerry's endorsement of this point of view and we would encourage the Central Bank to continue to embrace and recognise the value of these technological changes for organisations and their compliance officers.

Fintech/Regtech is an area of focus for the ACOI this year, particularly in bringing solution providers and compliance officers together. We will have a number of other events throughout the year so watch this space.

That point of driving cultural change within organisations brings to mind the continued evolution of the role of the compliance officer.

The ACOI has never seen the role of the compliance officer as merely "box ticking" champion within the organisation. The increasing regulatory obligations placed on organisations and the overt focus from some regulators and indeed organisations on "just" regulatory compliance can tend to place the function in a certain place in the mindset of boards/regulators and indeed some who work in the compliance profession

Please don't misunderstand me; regulatory compliance is a key area of focus. However it is not all that compliance officers should and can do. If all we've learned from the recent financial crisis is that more rules/guidance/regulation is what will make things better then we've missed an opportunity. If, however, we believe that the cause of the crisis at its core was indeed a failure of culture and behaviour from all stakeholders then influencing and changing both culture and behaviour has to be the greater goal. Compliance officers are perhaps uniquely positioned to do this with the support of boards and particularly independent non executive directors (INEDs).

"Fintech/Regtech is an area of focus for the ACOI this year, particularly in bringing solutions providers and compliance officers together. We will have a number of other events throughout the year so watch this space."

The challenge for compliance officers is however to stand up and be counted in this endeavour, to understand the businesses you work with and in, recognise the challenging goals your boards face both commercially and culturally and to put your hand up.

The regulator has told ACOI it will assist in driving this agenda with the compliance profession and we, the ACOI, have asked them to particularly make this point to the community of INEDs who sit on our organisations boards, as the INED is in many cases one of the most useful resources for the compliance officer.

ACOI has launched a programme of events starting with AML in January 2018 to continue to build bridges between the INED community and the compliance profession.

To make this "alliance" work both parties need to understand their individual roles and responsibilities but also how they can help each other add value to the organisations they work for. Regulators however also need to understand they need to play their part in both understanding the positions of INEDs within organisations, particularly in their expectations of INEDs, but also in understanding the role of compliance officers within organisations and challenges they face.

The PCF regime for compliance was largely welcomed but I'd ask the regulator to perhaps take a step back and Please Collaborate Further to ensure they understand and appreciate the role of compliance within organisations so we both get what we want and need and truly raise the standards higher within organisations and not simply tick more boxes. The ACOI is here to help in any way we can.

A final word on culture. Culture is often spoken about in the abstract, or purely in the context of the group or "organisation". Let's not forget culture within organisations, or nations or within groups or indeed of what's generally acceptable in society comes down to us, people, individuals.
To drive cultural change requires many things including personal accountability and responsibility. In that context I believe that we would be better served if there was more focus on truly holding individuals to account particularly when issues emerge.

If we are to truly grow and, in some cases, grow up as individuals, as a society and indeed in industry, personal accountability in both public and private life has to mean something.
In regulated industry, if that requires the greater use of individual sanctions for inappropriate or worse actions and behaviour, in order to drive cultural change then so be it – that may be the price to be paid and one that's worth paying.

I encourage you to continue to reach out to the Association as we continue to be the voice of compliance and of you our members

I look forward to hearing from you with your views, your offers of help, suggestions and thoughts on the future direction of the ACOI – all welcome. ICQ

Clive
March 2018.

IRELAND'S FINTECH OPPORTUNITY

With over 9,000 people working in the Irish Fintech sector, the outlook is very bright. With emerging technologies like blockchain now becoming mainstream, there will be both challenges and opportunities, writes Richard Walsh.

"Fintech' in its broadest sense, can be described as an activity, which brings together financial services, innovation and new technologies."

In 2017 Fintech reached a tipping point and is now poised for mainstream adoption across almost all major markets. By focusing intently on the customer proposition and leveraging technology in novel ways, Fintech firms are gaining traction and in the process are blurring boundaries between financial products and lifestyle propositions, as well as defining new standards within financial services.

Increasingly sophisticated consumers are drawn to Fintech services because propositions are simpler, convenient, transparent and readily personalized. This has had a ripple effect across the industry as consumers come to expect these characteristics of all financial products and providers, whether in retail banking, wealth management or insurance

Fintech firms are establishing themselves not only as significant players in the industry, but also as a benchmark for financial services. Their use will only rise as Fintech awareness grows, consumer concerns fall, and technological advancements, such as open API - Application Programming Interface , reduce switching costs.

Established financial institutions are faced with increasing costs of regulation and shrinking revenue streams. Their current propositions are being "unbundled" and "rebundled" by new and more nimble firms resulting in the disruption of traditional customer relationships. However, this dynamic has also created opportunities for collaboration between start-ups and established firms .Many examples are emerging of exiting providers with large customer bases, working alongside firms with new technologies who are keen to reach new users, bringing mutual benefits to all stakeholders.

What is Fintech?

'Fintech' in its broadest sense, can be described as an activity, which brings together financial services, innovation and new technologies. An obvious example is the use of smartphones to make payments, make investments, buy foreign exchange, obtain credit or even to buy cryptocurrencies. More complex back-office software applications such as artificial intelligence, RegTech and big data also fall under the definition of Fintech.

Various start-ups have been involved in the process of creating these new technologies, but many banks have also developed their own Fintech capabilities and have established in-house 'innovation labs' which concentrate on exploring new opportunities that both technology and indeed legislation such as Payment Services Directive 2 - PSD2. have brought about. A number of international Financial Institutions have selected Ireland for their Global FinTech endeavours including Citi Group, Credit Suisse, PayPal, MasterCard, and Accenture.

Fintech Globally

Strong investment of US$8.7bn in Q4 of 2017 propelled global Fintech funding over the US$31bn mark for last year, sustaining the high level of investment seen in 2016, according to the KPMG Pulse of Fintech Q4 2017 report. This brings the total global investment in the Fintech sector over the past 3 years to US$122bn.

"Both InsurTech and Blockchain saw record levels of Venture Capital investment this year, with InsurTech alone accounting for $2.1bn across 247 deals and Blockchain accounting for $512 million of investment across 92 deals", according to the report.

Geographically, the US accounted for almost two-thirds of global Fintech investment in Q4'17. In Asia, Fintech investment moderated to US$748M for Q4'17, while investment in Europe rose above $2bn in Q4'17, highlighting the region's growing maturity with respect to financial innovation and the ongoing evolution of numerous innovation hubs.

Interestingly, the countries with the greatest consumer adoptions are not necessarily the countries with the most active Fintech sectors.

The recent EY Fintech Adoption Index 2017 which looked across 20 markets found that many of the countries gaining a reputation for Fintech are below the average when it comes to consumer adoption of Fintech.

It should be said that the report only focused on consumers who had a smartphone, but Ireland coming 16th implies we have some way to go in driving adoption at home. And this might be about to happen. The same report predicts that Ireland's adoption will double in the coming years to over 52% as the 'early majority' start to adopt Fintech services. This growth rate is the highest of the 20 markets surveyed in the EY report.

Irish Fintech

In just over twenty-five years, Ireland's International Financial Services Sector has developed into a major player on the global financial stage. Across Ireland, almost 40,000 people are now employed in the Sector, and over 9,000 people work in Fintech. Today, there are over 200 foreign-owned and another 200 Irish-owned financial services companies spread throughout Ireland, delivering a broad spectrum of international financial services, with IDA Ireland and Enterprise Ireland playing an active role in development and support services.

While Ireland is strong in financial services, it is technology where we really punch above our weight. The Technology Sector employs

"While Ireland is strong in financial services, it is technology where we really punch above our weight. The Technology Sector employs over 100,000 people and includes 9 of the top 10 Global Tech companies."

over 100,000 people and includes 9 of the top 10 Global Tech companies such as IBM, Microsoft, Oracle and Intel. All the top ten 'born-on-the-internet' companies such as Google, Facebook, Airbnb and LinkedIn have also based their European Headquarters in Ireland, many in Dublin's Docklands area.

All parts of the eco-system exist, ranging from start-ups to scaling indigenous companies and multinationals, all of which are supported by Government policy that has identified Fintech as a key strategic area. Financial services companies already in Ireland with a significant technology presence include Citi, MasterCard, Aon, Fidelity, Prudential, Deutsche Bank and UnitedHealth Group.

Ireland enjoys the advantage of having the youngest population in Europe with 40% of our people under 29 years of age. It's a bright and a brilliant generation – educational achievements among the 25-34-year-old rate significantly higher than the OECD average. Already, a strong track record exists of Irish entrepreneurs building and scaling successful indigenous Fintech companies. Realex, Fexco, Fenergo, Fintrax and Corvil are just some of the Irish companies that grew up in Ireland and continue to expand globally.

Irish Domestic Fintech Companies

Ireland has good reasons to see Fintech as an industry where it can lead the way on the world's stage provided careful thinking goes into the preparation and the positioning of our advantages. To this point, the Governments International Financial Services 2020 (IFS2020) when published by then Minister Harris in 2015 was seen as a unique and skilful approach to the development of a thriving Fintech Sector.

What made the strategy unique was that, while being a Public-Sector initiative, it looked to the Private-Sector to devise the actions and objectives required to develop Ireland as a Global Fintech centre. This gave companies, both domestic and international who are heavily vested in Fintech, an opportunity to shape the ecosystem

and have their recommendations incorporated into the national plan.

Also important to Ireland are the potential opportunities Brexit Fintech brings about. As the prospect of a Brexit in which UK financial services companies lose their pan-European passporting rights becomes more real, we're seeing financial services companies authorised in London searching for alternative locations, and Ireland is high on that list. While regulators are pushing major banks and insurers to come up with a Plan B, Fintechs haven't had to be as quick to make decisions. But expect to see Fintechs increasingly examining their options over the next six months. And Ireland is now regarded as a key location for Fintechs looking to scale their businesses.

Ireland is one of a very few locations with a proven track record both in Financial Services and Technology, and a highly skilled talent pool of Fintech practitioners, many of whom learned their trade in the Digital giants and multinational banks who are based in Ireland.

This was the reason HubSpot CEO, Brian Halligan, gave for locating its European Headquarters in Dublin in an interview with SiliconRepublic. "One thing for certain is Dublin is the scale-up centre. All the companies are getting scale and HubSpot is one of them. Fast-expanding companies are crazy if they don't come to Dublin, in my opinion."

He has a point. Google came to Dublin in 2003 to create a small office of around 80 people and now it employs 6,000 people, making it the city's largest employer. Facebook also came to Dublin to create around 80 jobs in 2008 and now stands at over 2,200 people, with plans for 800 more. The same rate of growth has been experienced by companies like Airbnb and Twitter.

"Ireland has good reasons to see Fintech as an industry where it can lead the way on the world's stage provided careful thinking goes into the preparation and positioning our advantages."

Commenting on the density of talent now based in Dublin, Halligan said "We keep giving our global promotions to Dublin because the people earn them. What is interesting about the people who have been promoted is that they have come from companies like Google, LinkedIn and Salesforce – big scale internet companies. We are based in Boston and it is very hard for us to recruit someone from Google in California or from Facebook or Salesforce with the scale experience we need, but here in Dublin you can find them just across the street. That expertise is hard to acquire, and Dublin has acquired it."

The Regulatory environment is another important factor influencing the development of Ireland as a Fintech Hub. While we must not stop working to restore the reputation of financial services neither can we ignore emerging differences in the regulatory and licensing regimes faced by Fintech industries in competing jurisdictions.

Competing centres of Fintech such as London, Israel, the US and Asia enjoy regulatory systems that are arguably more growth focused than in Ireland and the EU. In conjunction with industry both the government and the regulator will need to modernise Ireland's regulatory environment and work at EU level to ensure that the EU's approach to regulating Fintech is based on promoting growth and modernization of financial services across the EU. In this regard, the sector is following closely developments at EU level in relation to Fintech, and in particular the work of the European Commission and the European Supervisory Authorities.

What's next for Fintech?

Investment is expected to remain strong as we go through 2018, with growing investor interest in regulatory technology (Regtech), artificial intelligence (AI) and Internet of Things (IoT) enablement. Blockchain technologies will continue to command a significant amount of attention. With some indications that production-capable blockchain solutions may be closer than envisioned, financial institutions are increasingly working to understand and leverage the potential advantages this technology brings.

The implementation of PSD2 in Europe is also expected to generate attention from regulators globally as they look to develop their own frameworks for open banking.

The prevailing wisdom about the nature of bank-Fintech relationships

has changed – from one of competition to one of collaboration. The potential for a win-win is certainly there, suggests Gavin Kelly, newly appointed CEO of Retail Ireland at Bank of Ireland. "What's key for me is not to be afraid of innovation, but to partner with Fintech companies and to partner with new ideas," he told Finextra in a recent report. "We have a lot of experience in the banking industry, particularly in areas such as regulation, and we've got significant customer bases. We also have trust. So, what we've got to do is use our strengths and to partner with new, innovative Fintech companies to provide better solutions for our customers."

One area with real potential for cooperation between banks and Fintechs is Payments. PSD2 and open banking, digital identity and GDPR all require technology investment by the incumbents, much of which is similar – and all feed into an emerging bigger picture underpinned by a new approach to payments infrastructure. It can be helpful to think about how rapidly the smartphone landscape has developed during the past two years. If a bank's systems can't support real-time, any-to-any connectivity and open APIs, then where does that bank think it will be in five years?

The payments industry needs to focus not just on the bit it does well already – the reliability and the resilience – but also on the data. Overall if the payments industry doesn't wake up to the fact that it's the data that is more important, then it risks becoming irrelevant.

The payments business is an enabler for Fintech and is the banks' value-added element. Payments are intrinsic and inextricably bound to digitalisation and can be the banks' secret weapon to stay relevant. In the Uber example, the pain of the payment has been eliminated. Customers still must pay for their taxi ride but now the ride is disassociated from the payment. The payment process is never pleasurable. If the banks can make it invisible they will have a ready partnership with many Fintechs.

It could be said that banks' adoption of Mobile Banking was in many respects the first large scale, successful embodiment of fintech in the provision of financial services to consumers. That points to the capacity of banks to be both responsive and innovative. ICQ

Richard Walsh, Head of Digital & Payments, Banking & Payments Federation Ireland.

CLOUD COMPUTING

CONSIDERATIONS FOR SECURE ADOPTION

As the world becomes more and more connected, organisations are increasingly adopting cloud-based services to meet their business needs.

Cloud computing can be defined as the use of a network of remote servers, hosted on the Internet, to store, manage and process data, rather than a local server or a personal computer. It is a game changing technology which is driving and will continue to drive cost reduction and innovation across organisations. The diagram below depicts the different cloud computing service models, the essential characteristics lane showing clearly the advantages of each of the service models, in particular Software-as-a-Service (SaaS) applications have created today's work-from-anywhere culture, giving us the ability to securely access work from any device. While the potential benefits of cloud computing are compelling, the use of cloud computing services is driving new risks, security and privacy concerns, and opportunities that impact all elements of the business ecosystem. There is no doubt that organisations need a strategic, flexible, and end-to-end security, risk, and compliance capability to enable secure cloud transition and business cloud transformation.

Furthermore regulators are becoming increasingly more interested in cloud computing. It is understood simply as a version of IT outsourcing and with that comes legal and regulatory requirements that must be monitored, reported and adhered to. As part of cloud adoption and transformation, organisations must identify and prioritise

"While the potential benefits of cloud computing are compelling, the use of cloud computing services is driving various new risks."

threats and risks; then design, implement, and operate risk and cost-appropriate controls to address them. Legacy security, risk, control and compliance capabilities are not sufficient to address cloud risks. Organisations must evolve their security, risk, control and compliance capabilities to enable cloud transformation of the business and benefits realisation. It is good practice to ensure that an organisation's cloud security capabilities address these key guiding principles:

Business & stakeholder mindset

Legacy security mindsets won't work; security must operate with an agile business risk advisory mindset with understanding of cloud architecture and operations. Cloud is fundamentally changing all aspects of the digital business ecosystem. Security focused on technology will fail to deliver the required benefits. Security must meet the current and enable future needs of a broad rang e of stakeholders.

Risk focused

Security exists to reduce business risk; cloud security must enable and provide solutions to understand and reduce risks to acceptable levels. Existing capabilities are often insufficient to address new cloud security risks. A continuous threat and risk management capability and secure operations capability should be developed for current and planned cloud deployments.

Protect cloud

Cloud security architecture and solutions should address security across multiple levels and use cases: ***IaaS*** (Infrastructure as a Service Provider); ***PaaS*** (Platform as a Service); ***SaaS*** (Software as a Service).

Cyber and privacy compliance

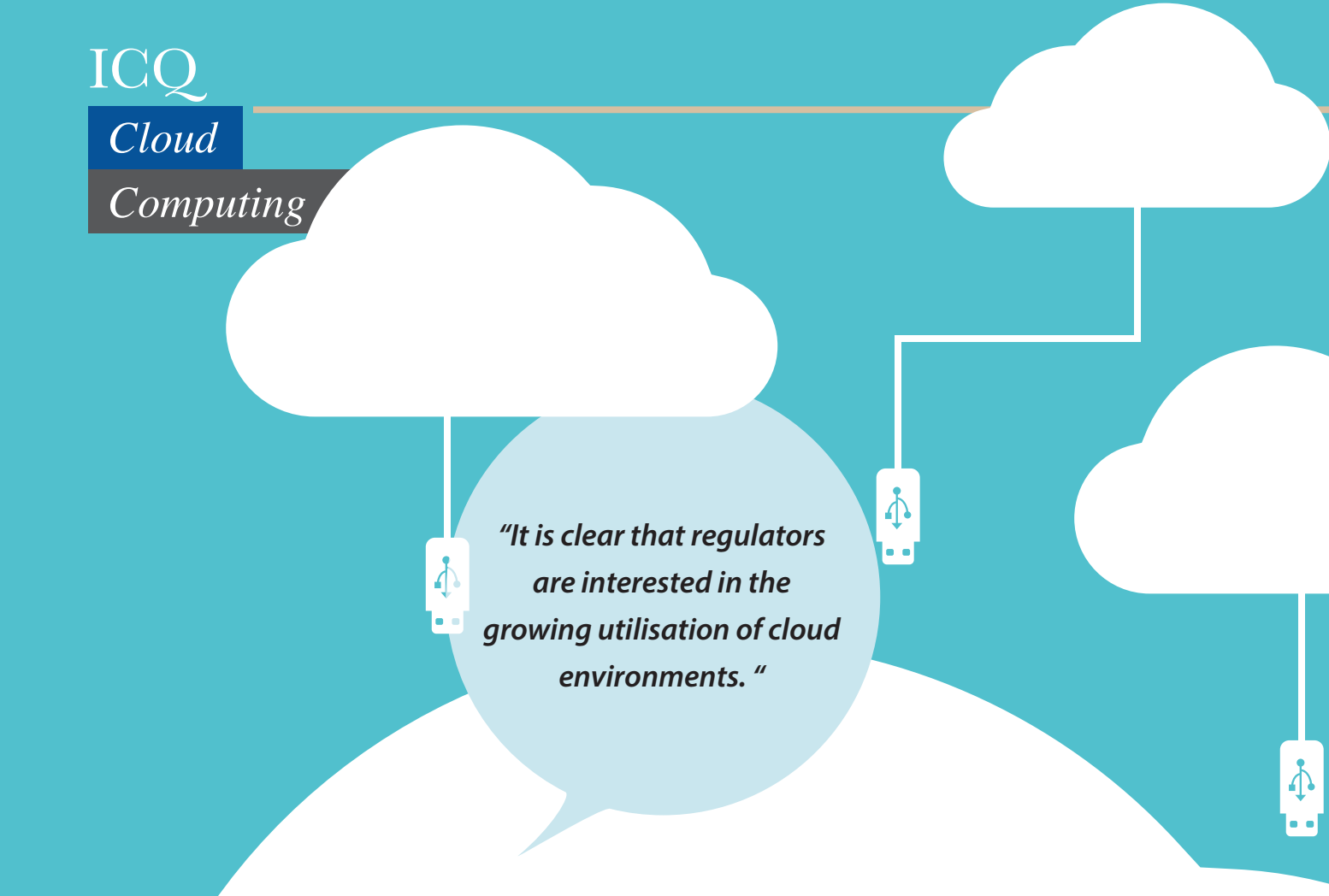
Cloud security capabilities should be implemented, and operated to demonstrate and enforce cyber and privacy compliance to appropriate frameworks and regulations. Cloud adoption and transforma tion will likely mean expanding the use of third party suppliers and collecting, storing, and transacting user data across geographic and political boundaries. Organisations are responsible for ensuring compliance and protection of user data across the global landscape. The Cloud security strategy must include how the organisation will achieve and maintain compliance to privacy laws, principles and regulations.

Agile, on-demand &, seamless

While security fundamentals still apply, the security technology, process, people and delivery models must adapt to enable cloud adoption and operations.

Invest smart

Legacy investments are not enough; agile, APIdriven and purposebuilt solutions for cloud are required (e.g., security as a service).



"It is clear that regulators are interested in the growing utilisation of cloud environments. "

There are many industry leading control frameworks that can be adapted to ensure organisations are managing the risks associated with cloud computing. Cloud security should align to common control domains as those addressed in leading control frameworks such as CSA, NIST, ENISA, and ISO*.

The Central Bank of Ireland released guidelines in September 2016 that deal with IT Outsourcing Risk (including cloud service providers [1]) and these should not be ignored in the context of outsourcing to the cloud, in particular the requirement to have completed adequate due diligence and the requirement to have appropriate contracts in place with cloud service providers. In addition the European Banking Authority ("EBA") have recently released a set of recommendations specifically relating to the reporting and monitoring requirements of organisations that are outsourcing to the cloud [2]. The principle of proportionality should be applied throughout the recommendations and the recommendations should be considered in a manner proportionate to the size, structure and operational environment of the organisation as well as the nature, scale and complexity of its activities [3].

The recommendations include guidance on the security of the data and systems used. They also address the treatment of data and data processing locations in the context of cloud outsourcing. Organisations should adopt a risk-based approach in this respect and implement adequate controls and measures such as the use of encryption technologies for data in transit, data in memory, and data at rest.

It is clear that regulators are interested in the growing utilisation of cloud environments. Financial Regulators will not be the only bodies interested in cloud computing, come May 25th this year, all European Data Protection Regulators will also have a keen interest in cloud outsourcing especially around the due diligence procedures carried out in advance of employing a cloud providers to ensure that the personal data they hold for organisations is protected, secure and in compliance with all aspects of the General Data Protection Regulation ("GDPR"). This does not mean that Regulators are not averse to cloud computing however their new and continued increased focus on the area of outsourcing means that that organisations must ensure they manage the risks associated with cloud computing to address the regulators' expectations.

The following table summarises some of the areas of focus and regulator expectations. All areas should be included in scoping and those most relevant to your cloud journey should be selected for assessment.

[1] CBI Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks (Outsourcing Guidelines). [2] Final report on recommendation on cloud outsourcing EBA/REC/2017/03). These recommendations apply to credit institutions and investment firms as defined in Article 4(1) of Regulation (EU) No 575/2013 (Capital Requirements Regulation - CRR). [3] This means that organisations must have a defined risk appetite in relation to its IT environment which will allow them to apply the principal of proportionality across defining appropriate risks and controls.

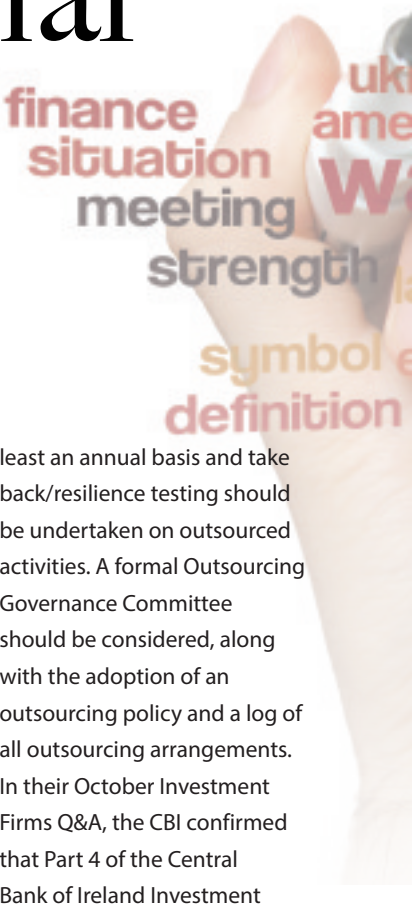
Area	Expectation
Cloud Security, Governance, Risk & Compliance (GRC)	• Identify regulatory, privacy and security requirements associated with the particular cloud outsourcing arrangement including the business process being supported • Implement a cloud governance and security framework incl uding the documentation of policies and procedures where appropriate
Cloud Strategy	• Define and document a cloud strategy ensuring overall business and IT Strategy alignment • Complete cloud service provider selection and sourcing due diligence procedures in line with organisation procurement and sourcing policies and procedures
Cloud Architecture and Integration	• Define system performance and interface requirements as defined by the relevant end user • Define cloud Integration Strategy • Understand and define application structure and placement
Cloud Migration	• In order to move services to the selected cloud provider smoothly, ensure there is a clearly defined migration plan and program governance in place to include people and process change management
Running Cloud IT	• Ensure adequate contracts are in place with documented and defined exit strategies, • Carry out regular performance assessments against defined key performance indicators to ensure the cloud service is providing adequate services as well as value for money • Ensure the right to audit clauses are executed on a regular basis

To summarise transitioning securely to the cloud is not a piece-meal, one-time endeavour. Organisations need to adapt a strategic, flexible, and well planned approach to enable cost-effective adoption of multi-cloud environments and business cloud transformation. Organisations need to ensure that the adaptation of a cloud environment is beneficial for them from a long term strategic perspective. It is now more than ever that it is crucial for organisations to have a fully aligned business and IT Strategy in place to drive the business forward in a fast changing technological world . ICQ

"Organisations need to adapt a strategic, flexible, and well planned approach to enable cost-effective adoption of multi-cloud environments and business cloud transformation."

Managing Financial Sanctions *Risk*

FUNDS WORKING GROUP



Central Bank Guidance on Fund Administrator Outsourcing

The ACOI Funds Working Group hosted a Regulatory Update on 21 November 2017, at which Niamh Mulholland, KPMG, delivered a presentation on Outsourcing Arrangements of Fund Administration Activities. Attendees were informed that the Committee of European Banking Supervisors' ('CEBS') Guidelines on outsourcing set out the key principles for outsourcing by financial services firms and have been the reference point for a pan-European approach. Sectoral approaches have emerged, however these approaches are largely based on the CEBS principles. Central to the oversight of fund administrator outsourcing arrangements is the requirement to demonstrate control over the outsourced arrangement, and to mitigate the associated risks that include:

- **Concentration Risk:** whereby a market or industry segment becomes over dependent on a few service providers.
- **Governance & Oversight** Risk: that stems from firms not taking reasonable steps to oversee the outsourced function in an effective manner and to ensure that the outsourced service does not have a negative impact on clients.
- **Contingency Planning Risk:** the risk associated with the potential failure of the outsourced provider and the impact this could have on the regulated firm which could be largely unprepared.
- **Substance:** the Central Bank of Ireland has articulated the perspective that a challenge will be present where a firm seeking authorisation in Ireland that plans to delegate or outsource substantial activity to the extent that there is nothing more than a "letter box entity" in Ireland.

To achieve this level of oversight, core management functions should not be outsourced, and the fund administrator must continue to exercise adequate and effective control and decision making. The outsourcing should not impair the ability of internal governance, such as compliance and internal audit functions, to oversee and review the arrangement. In addition, a fund administrator is required to evaluate the performance on an ongoing basis, to include periodic due diligence related visits.

The regulated entity should ensure a clear relationship with third party service providers and/or intra-group entities, the Central Bank requirements apply equally to both. Mechanisms should be implemented to ensure effective governance and oversight of outsourcing arrangements on an ongoing basis e.g. receipt of relevant management information such as Key Performance Indicators, and an annual review of Service Level Agreements. Business Continuity Plans should also be reviewed and tested on at least an annual basis and take back/resilience testing should be undertaken on outsourced activities. A formal Outsourcing Governance Committee should be considered, along with the adoption of an outsourcing policy and a log of all outsourcing arrangements. In their October Investment Firms Q&A, the CBI confirmed that Part 4 of the Central Bank of Ireland Investment Firms Regulations apply to both Irish and non-Irish administered funds.

Key points to consider include:

- The extent to which periodic due diligence visits are conducted will be dependent on the nature, scale and complexity of the outsourced task.
- Where there is a change to existing outsourcing arrangements (save the addition of new funds) this must be notified to the CBI under Regulation 18. A Regulation 18 notification must also be made where there is a change of fund administrator.
- Fund administrators

must submit an annual return template on outsourcing to the CBI.

- All clients impacted by an outsourcing agreement must be notified in sufficient time before the commencement of any outsourcing arrangement.
- Staffing arrangements at the outsourced service provider should include training and ensuring that sufficient resources are in place. Resources should be identified as being (a) an Ireland dedicated team, (b) an activity dedicated team, or (c) an investment fund specific team.
- **Performance and Quality Standards:** Including detailed Service Level Agreements (SLAs), Standard Operation Procedures (SOPs) and Key Performance Indicators (KPIs), that are monitored and reviewed at least annually.
- **Oversight:** Details of the oversight conducted by the fund administrator of an outsourcing arrangement should be included in a Regulation 18 notification.
- **Business Continuity:** Where an alternative outsourcing service provider is required or an existing outsourcing service provider needs to change location, the fund administrator should assess what budget may be necessary if such an event occurs as a result of disaster recovery. This matter should be addressed in the context of the capital planning process and reference should also be made to such a stress test in the fund administrators outsourcing policy, business continuity policy or resilience testing policy.

"The regulated entity should ensure a clear relationship with third party service providers and/or intra-group entities, the CBI requirements apply equally to both."

In conclusion, outsourcing arrangements will continue to be an area of increased focus, and pre-approval of any outsourcing arrangement must be sought from the CBI prior to implementation. Adequate consideration should be given to ensuring that the appropriate risks and controls are in place, and that ongoing oversight may be demonstrated through measures such as those set out above. ICQ

The Funds Working Group would like to hear any feedback / comments that members have on this topic. Please send feedback to info@acoi.ie.

ICQ

Prudential Regulation & Governance

Working Group

TARGETED REVIEW

OF INTERNAL MODELS [TRIM]

The inspection process – PR&G Working Group. TRIM refers to the "Targeted Review of Internal Models" which is currently being conducted by the ECB.

TRIM refers to the "Targeted Review of Internal Models" which is currently being conducted by the ECB. The programme commenced in 2015 and is scheduled for completion by late 2018 (with potential extension to 2019). The programme was established in response to criticism of banks' internal modelling practices; specifically, in respect of observed variations in risk assessments and supervisory practices across jurisdictions and banks within the Single Supervisory Mechanism (SSM). The SSM refers to the system of banking supervision in Europe, involving supervision by the ECB in conjunction with the national supervisory authorities of the participating countries. The ECB directly supervises the 119 significant banks of the participating countries, with the decision on whether a bank is deemed significant or not being based on a number of criteria. This has implications for more than just banks too, in terms of the approach to the supervisory desire for understanding firms' modelling processes and systems.

Objective

The purpose of TRIM is to evaluate the adequacy and appropriateness of Pillar I models, as permitted under the Internal Ratings Based (IRB) approach. It also considers more general topics concerning model governance, internal audit and data quality. The review should improve the credibility of capital levels estimated by significant institutions through their internal models.
The review focuses on approved internal models for credit, market and counterparty credit risks. Significantly, operational risk models are deemed out of scope for the TRIM exercise – mainly due to the planned phasing out of the Advanced Measurement Approach (AMA) under Basel IV proposals.

The intention of TRIM is to achieve four main objectives, namely to:

- Ensure compliance of internal models with regulatory standards;
- Align supervisory practices across the SSM;
- Deliver a planned reduction in unwarranted variability in Risk-Weighted Assets (RWA); and
- Verify the adequacy of capital estimates arising from banks' differing interpretations of the regulatory requirements in internal model development.

Method

TRIM has been divided into two main components:

- **Preparation phase (2016 – 2017):** Includes prioritisation of models, methodology definition, project planning, field-testing and training; and
- **Execution phase (2016 – 2018/19):** On-site and off-site inspections, data quality reviews, consistency checks, peer reviews and supervisory recommendations.

One of the key elements of the preparation phase was the completion and submission of a detailed, standardised template by all significant institutions approved to use internal models. The template covered a broad range of topics, including model risk, model governance (including validation and approval processes) and model usage. The purpose was to (i) identify the critical models in scope for the review; and (ii) establish the plan for model assessments in the execution phase. The preparation phase concluded in early 2017.

The most onerous element of TRIM occurs in the execution phase. This comprises a series of on-site and off-site reviews of the internal models identified through the preparation phase.
For each individual TRIM inspection, a supervisor within the relevant national competent authority is appointed Head of Mission (HoM). This person is accountable for executing the inspection in line with the ECB's Guide for the Targeted Review of Internal Models (TRIM) (TRIM Guidelines)
The HoM is supported by an inspection team, which includes both supervisors and external consultants. For each internal model, the TRIM review broadly follows standard procedures similar to the ones set out in the ECB's Guide to on-site inspections and internal model investigations. These include:

- Submission of requests for data and documents;
- On-site visits by the inspection team, including interviews of bank staff; and

Off-site analysis, to include independent calculations, replications and data quality assessments.

Once the inspection is complete, a draft report is prepared, which outlines key findings and recommendations. This report is subjected to a quality assessment and peer comparison by the ECB Once these consistency checks are completed, the draft report is shared with the bank's management,

"The new methodologies will form the basis for future approval and on-going supervision of the internal models for significant institutions. interpretation of regulatory requirements."

to allow for meaningful review and challenge; this process can last up to two weeks, before a final exit meeting is held to conclude the inspection. Finally, a formal letter – outlining the agreed findings and recommendations – is issued to the bank.

In addition, the ECB (in conjunction with the national competent authorities) have established a number of centralised, specialist teams. These 'Centres of Competence' – alongside a 'Harmonisation Board' – have been created to support the HoMs in carrying out TRIM inspections. Their focus is primarily on overseeing the results of the inspections to ensure that appropriate convergence of model outputs is achieved.

An important feature of this centralised process is how on-going benchmarking of internal models is expected to be undertaken. Comparisons will be likely carried out against peer banks across the SSM. Therefore, internal models of Irish banks (which are assessed as part of TRIM) could now be benchmarked against those from peer banks across Europe.

Implications

The new methodologies will form the basis for future approval and on-going supervision of the internal models for significant institutions. This will include wider benchmarking of model parameters and a more precise interpretation of regulatory requirements. Consequently, significant institutions will have to demonstrate their positioning towards the principles set out in the ECB TRIM Guidelines and other related EBA Guidance. In addition, the methodologies are likely to inform the supervision of non-significant institutions by setting the standard of "good practice". In particular, TRIM's methodologies on governance, internal audit and data quality are likely to be applied in a proportionate way to other banks.

Also, supervisory engagement with banks on modelling and data issues is likely to lead to a significant increase in information requests. This will enable supervisory authorities to conduct data quality analyses and replicate critical calculations independently. Consequently, a bank's governance and documentation of data and models must be comprehensive and of sufficient detail to allow supervisors to apply this enhanced level of oversight.

Conclusion

TRIM will have a substantial impact for significant institutions within the SSM. The TRIM Guidelines will likely form the primary basis for future approval and on-going supervision of internal models. All significant institutions will have to demonstrate their positioning towards the "TRIM interpretations" of the requirements.

Non-significant institutions are likely be impacted. The TRIM methodologies on model governance, internal audit and data quality are likely to be viewed by supervisors as "good practice" to be applied in a proportionate way to all banks.

TRIM also demonstrates that inspections now increasingly involve off-site analyses by supervisory inspection teams. Consequently, banks' documentation has to be comprehensive so that supervisors can analyse data and replicate their calculations independently. In summary, supervisory practices continue to place a considerable burden on banks' data, modelling and compliance teams. ICQ

Adrian Toner, KPMG – Regulatory Team on behalf of ACOI PR&G Working Group.

KPMG

At the heart of business in Ireland

So What Is CORRUPTION?

So what is Corruption? Corruption, put simply, is any form of abuse of power for private gain.

Corrupt practices are used to illegally influence the behaviour of an individual in a decision-making role, in a company, an organization or governmental authority. Corruption can be wide ranging and take many forms, including bribery and fraud. It is not always a matter of handing over cash. It can involve anything of value, so long as it is intended to improperly influence a decision maker, for example:

- Jobs/internships for a public official or relative without merit or justification to gain contracts;
- Small, unofficial payments or 'grease' payments made to public or government officials to secure or expedite a routine government action (e.g. obtaining permits, processing visas or setting up services such as utilities);
- Hidden sponsorships/political/charitable donations with customers or vendors to maintain poor performance or services;
- Lavish, extravagant or inappropriate hospitality/entertainment to establish improper close links;
- Exotic foreign travel paid for by a supplier outside work to win business unfairly over the competition;
- 'Kickbacks' in the form of rebate or service fees to maintain underperforming vendors in your supply chain that find or maintain sales or customer leads;
- Underhand commissions to brokers, professional service providers or middle men to secure a new license or regulatory inaction……the list is endless……

Why is it Such a Big Deal?

In fact, corruption is such a big deal it has its own day each year; the December. 9th is International Anti-Corruption Day. And for good reason – according to the United Nations, a staggering $1 trillion changes hands in the form of bribes every year, while $2.6 trillion is stolen through corruption. The toll is serious – this crime undermines social and economic development around the world. In addition to harming our reputation, this type of activity also exposes us to inefficiencies, wasteful practices, fraud losses and civil and/or criminal liability and reputational damage. This can be hard and expensive to undo; companies and individuals may ultimately be disbarred from office or doing business in the private or public sector.

International Anti-Bribery and Anti-Corruption ("ABAC") Laws are Strengthening Everywhere to Prevent Corruption

There are new laws in many countries this year including France, Argentina, and Ireland. Businesses are coming under increased scrutiny to ensure their domestic and foreign operations comply with anti-corruption and anti-bribery legislation. The risk of investigation has never been greater and the reputational risk, given the current media interest in these sorts of scandals such as the Panama Papers, 1MDB, Rolls Royce and the recent political upheavals with the House of Saud will increasingly be a consideration for companies, especially publicly traded ones or companies pursuing financing

or other significant transactions abroad. This is especially important given the extra-territorial effects of International ABAC Conventions most countries, including Ireland, have signed up to in the global fight against corruption. Countries like Brazil have enacted new far reaching anti-corruption measures to prevent corrupt activities such as ticket touting at International sporting events like the World Cup and the Olympics. Ireland is modernizing its laws too by creating a single comprehensive ABAC law that will be similar in scope to the UK Bribery Act and extend corrupt offences to all corporate bodies and individuals in both the public and private sector, including the financial services industry. The U.S Department of Justice ("DOJ"), the Securities and Exchanges Commission ("SEC") and the Serious Fraud Office ("SFO") in the UK continue to focus on the financial services industry and on joining forces to prosecute Multinationals. Citigroup is currently under investigation for alleged improper hiring practices similar to Morgan Stanley and Standard Bank in the past for providing jobs to the relatives of government officials in Asia and hidden commission payments in exchange for business involving large capital infrastructure projects in Africa. 2017 saw a record year for corporate criminal enforcement actions for bribery/ corruption, resulting in $822 million in corporate criminal fines, penalties, and forfeiture, and total enforcement action amounts payable to U.S. and foreign authorities of $2.5 billion. Study these cases in detail as the learnings are applicable anywhere you do business, irrespective of your perception or experience of the risk environment where you operate and do business.

The US Experience

In the US also, the Department of Justice ("DOJ") has extended the Foreign Corrupt Practices Act ("FCPA") Pilot Program in March 2017 to continue to motivate companies to self-disclose misconduct and cooperate in investigations to secure reduced penalties. Over 120 companies have self-disclosed investigations already this year, in financial services, waste management, tobacco, education, food production and most notably, tax preparation services as well as the extractive industries (oil, gas and mining) and even the renewables sector; this is an important development for Irish Companies operating in the US and worldwide. This shift in approach by US Regulators and related guidance in the form of the new Corporate Enforcement Policy is worth reviewing because many International companies use

Europe and the U.S as a launch pad to operate in third countries because of the lower tax base, scale and developed nature of these markets. The pilot program guidance provides a useful framework for benchmarking and self-assessing risk and ensuring the global footprint of your business has appropriate and proportionate companywide ABAC procedures in the event of a bribery occurrence abroad. Being in a position to show how you are complying with this Guidance could be a key defense in securing any declination in prosecution and reduced penalties. This is because the guidance indicates for the first time 'a safe harbor' for having a robust compliance program; that said, there are no such similar safe harbors with domestic legislation here in Europe; in fact the opposite is true and there is a strict liability 'all bets are off' offence here in the event of a breach, irrespective of whether or not there is a compliance program in place.

The Irish Response to Bribery and Corruption

Remember, bribery and corruption can materialize anywhere, irrespective of country, industry or target market. Don't be complacent and focus solely on third world countries with poor human rights records or on bribe payer or corruption percentages indices from Transparency International. Take Ireland as a case in point. On 2 November 2017, the Government published a package of measures designed to strengthen Ireland's response to white collar crime. The package contains 28 measures, each with a specific target date for completion. It also published the long awaited Criminal Justice (Corruption Offences) Bill 2017. Following a recommendation made by the Mahon Tribunal, the new Criminal Justice (Corruption) Bill, will makes it an offence for public officials to use confidential information acquired in the course of their duties to obtain an advantage. It also outlaws a person giving a gift or advantage where the person knows, or ought reasonably to know, that it will be used to facilitate corruption.

"Remember, bribery and corruption can materialize anywhere, irrespective of country, industry or target market."

Irish Anti-Bribery and Corruption Laws Are Modernising this Year to Catch up

Complex and outdated Irish Anti-Bribery and Corruption laws are being modernised this year by the Government's Department of Finance, the Department of Justice and Equality and the Department of Business, Enterprise and Innovation, following political pressure internationally from the Organisation of Economic Co-operation and Development ("OECD") and the Group of States against Corruption ("GRECO") over the low levels of prosecutions and penalties and sanctions. When the new laws come into force (expected in late 2018), it will be an offence to 'corruptly' offer or give (or accept or obtain) a gift, consideration, or advantage to a person as an inducement or reward for them doing something in relation to their office, employment position or business. 'Trading in influence' or the promise of an undue advantage to someone who either attempts to or exerts improper influence over a public official's decision making will also be illegal. The use by any public official of 'confidential information' obtained in their role to corruptly obtain a gift, consideration or advantage will also be criminalised. It will also be an offence to 'knowingly or otherwise' give a gift, consideration or advantage to facilitate corruption, with the burden of proof resting on the offender with any benefit forfeited by the state. This is a powerful and potentially far reaching provision for C-suite directors, beneficial owners and other key business influencers such as Pre-approved Controlled Function ("PCF") and other Controlled Function ("CF") role holders making strategic, commercial and compliance decisions in newly regulated and rapidly expanding businesses, where the nature of the roles may present a conflict of interest. This may be especially important for new payments services businesses with extensive shared services or

undocumented outsourcing and remuneration arrangements in contracts with fintech companies. 'Corruptly' creating or using 'false documents', or threatening harm to a person, in order to induce or influence them to do something in relation to their office, employment, position or business will also be illegal. Sentences can be up to 10 years and unlimited fines, disbarment from bidding on procurement contracts and disgorgement of company profits.

Section 18 of the Criminal Justice (Corruption Offences) Bill 2017, is worth close examination. It provides for the criminal liability of a corporate body where a director, manager, secretary or other officer, employee or subsidiary (both here and abroad) commits an offence with the intention of obtaining or retaining business or an undue advantage in the conduct of business for the Corporate Body.

This section goes even further is so far as it seeks to go behind the company itself to the person who is "pulling the strings" and who committed the offence. Where the improper business activity was committed with the consent, connivance or wilful negligence of an individual (including a shareholder or director), they too can be held personally liable. They can also be removed from office or holding a position of power (including directorships) for 10 years.

To avoid conviction and fines there is a key defence open to the corporate body that it took all "reasonable' steps" and "exercised all due diligence measures" to avoid committing the offence. Therefore, it will be imperative for companies to put in place strong ABAC programs and communicate policy requirements and train all staff.

Some Strong and Weak ABAC Compliance Practices for Your Business to Consider

Having an ABAC compliance program that aligns with other aspects of your Operational Risk Management Framework will be a key defence against a regulatory breach or bribery threat when the new laws come into force. Companies and individuals tasked with ABAC accountability must properly identify your ABAC risks and controls up front in your Risk Management Framework. Producing monitoring and reporting key performance Indicators to show ongoing sustainability of your ABAC Internal Control Environment is vital. Organisation must be able to demonstrate a simple, repeatable, efficient and effective compliance program and underlying business processes that uses procedural documentation, experiential information and good data governance to prevent corruption.

Here are some practical tips to help you develop or assess your ABAC Compliance Program before the new laws come into force and in preparation for Anti-Corruption Day on the 9th December:

1 Demonstrate Top Level Commitment and Accountability for your ABAC Program from Day 1.

STRONG PRACTICE

- Assign ABAC Compliance to a single senior individual with relevant subject matter expertise in employee and third party conduct risk management. The individual should have direct access to the Board(s) of operating legal entities and voting rights on sub Risk Committees, such a Fitness and Probity, Sales and Service Practice Remuneration, Fraud, Conduct of Business, Ethics and Third Party Risk oversight Committees and participate in other committees to identify useful sources of data (e.g. Customer Complaints, Training Committees) that may be indicative of corruption.
- Board and Risk Committee approved ABAC Policy in place and ABAC laws tracked through regulatory and policy change processes and communicated and assessed for gaps in business line procedures and controls.

WEAK PRACTICE

- Assigning ABAC Compliance to the AML/ CFT or Compliance Functions where those programs are principally customer conduct risk focused and there are conflicting regulatory priorities and shared resources and no ABAC SME.
- No annual bribery risk assessment undertaken where inherent risks, the regulatory environment, controls and residual risks are not rated.
- No research is done to articulate technical and material breach scenarios and their likelihood of occurrence across different legal entities, employees, business lines, joint venture, mergers and acquisitions activities, financial products, and outsourcing and vendor services and in different jurisdictions with licensing or regulatory obligations.
- Where risk is not assessed, a reactive approach is taken where no corruption investigation or event management and external materiality reporting protocols are put in place for oversight committees to follow in the event of an employee fraud or bribery instance.

2 Demonstrate the Recording and Delivery of ABAC Training and Awareness Communications.

STRONG PRACTICE

- Develop and track the number/ percentage completion of ABAC training and any follow up awareness communications assigned to employees and higher risk individuals ("PCF's/ CF's") electronically through established Learning Management Systems and WebEx Training Tools.

WEAK PRACTICE

- No training completion rates presented to Training Oversight Committees or an equivalent oversight forum,
- New training not refreshed with lessons learned year on year or role based training.
- Training not delivered to key business influencers, including directors, officers and managers on their legal and personal liability risks.

3 Demonstrate that gifts, travel and entertainment are reported, reviewed, rejected and escalated and there is independent oversight.

STRONG PRACTICE

- Develop gifts, travel and / entertainment categorisation and reported within your Finance/ Corporate Payables systems. Place material thresholds for reporting and set limits for lavish or extravagant entertainment that is too frequent with the same parties and be indicative of improper close personal links.
- Monitor rejects and escalations with Second Line of Defence oversight from Ethics or Compliance or Audit Committees for Senior Managers regularly 'at higher risk' business lines like wealth management or wholesale banking or commercial insurance that may be regularly entertaining clients or vendors.

THE ACOI NEEDS YOU!

The ACOI is a membership-led organization and we need *your* help!

Our working groups are comprised of members volunteering their time and expertise to help the ACOI be the go-to place for compliance officers in Ireland.

APPLY BELOW TO JOIN A WORKING GROUP

To ensure that each Working Group has the broadest skill set possible and is working to provide the most up to date information for ACOI members, we are inviting expressions of interest from all members to join a working group!

Each Working Group run a number of events, comprised of lunchtime seminars and workshops. Events are built around hot topics concerning each Group's particular area of expertise and are CPD accredited. Working Groups also contribute content for the ACOI's quarterly publication, ICQ, related to events they have hosted or developments in the compliance sector.

ACOI CURRENTLY HOST THE FOLLOWING WORKING GROUPS:

- AML
- Consumer Protection
- Credit Unions
- Funds
- DP & Technology
- Pensions
- Prudential Regulation & Governance
- Regtech

Any ACOI member who wishes to express an interest in joining one of our Working Groups can do so by *clicking* the link below.

https://www.acoi.ie/working-groups/

WEAK PRACTICE

- Internal Travel & Expense processes not supplemented with the ability to record gifts received by employees from third parties resulting in no passive bribery risk tracking.
- Names, job titles of individuals and types of companies and industries, corporate bodies, government agencies and purpose of expenditure using company funds not documented and no supporting itemised receipts in Travel & Expense Management systems.

4 Demonstrate the identification of higher risk third parties and termination for bribery/ corruption issues.

STRONG PRACTICE

- Using complaints data in annual risk assessments as a source for identifying improper sales and services practices that could potentially result in bribery risk materializing.
- Mandatory due diligence on vendors from both the public and private sectors in a centralized system of record. Risk rating and Politically Exposed Persons ("PEP") screening their beneficial owners/ controllers and performing negative news searches on 'at risk 'vendors before paying invoices through your Finance/ payables processes. Doing spot checks on service rebates outside your regulatory footprint or to fourth parties.

WEAK PRACTICE

- Corporate Bodies, Government Agencies or Professional Services Firms such as Accountants, Lawyers or Tax advisors exempted from Company Vendor Due Diligence Programs and approvals or policy exemptions sought by their relationship managers for related invoices through budgetary or third party pre-approval or downstream accounts Payable processes.

5 Demonstrate clear ABAC incident identification/ escalation processes.

STRONG PRACTICE

- Properly assigned ABAC risk oversight to individuals in lines of business with fraud or operational risk roles. Escalation and monthly reporting routines to a centralised Second Line of Defence ABAC or Finance Function covering gifts and potential policy violations, or other proportionate procedures, dependant on the size, nature and scale of your business.

WEAK PRACTICE

- No anonymous or confidential whistleblowing or ethics hotline in place and or no escalation or reporting routines for ABAC Violations from the in house or vendor hotline to relevant oversight committees.
- Customer AML SAR escalation processes being used to refer confidential employee and third party ABAC referrals where no AML Risk is detected.

6 Demonstrate that political and charitable contributions are not improperly or illegally made to gain or retain business for the company.

STRONG PRACTICE

- Political and Charitable Contributions Governed by Strategic Business, Vendor Management and Corporate Payables Policies. All contributions approved independently and appropriately tracked and reported through monthly escalation processes.

WEAK PRACTICE

- No ability to categorise expenditure as political or charitable donations associated with a particular customer or vendor relationship in related approval systems, books and records.

7 Demonstrate the identification and screening of higher risk employees and that disciplinary actions are taken for bribery/ corruption issues.

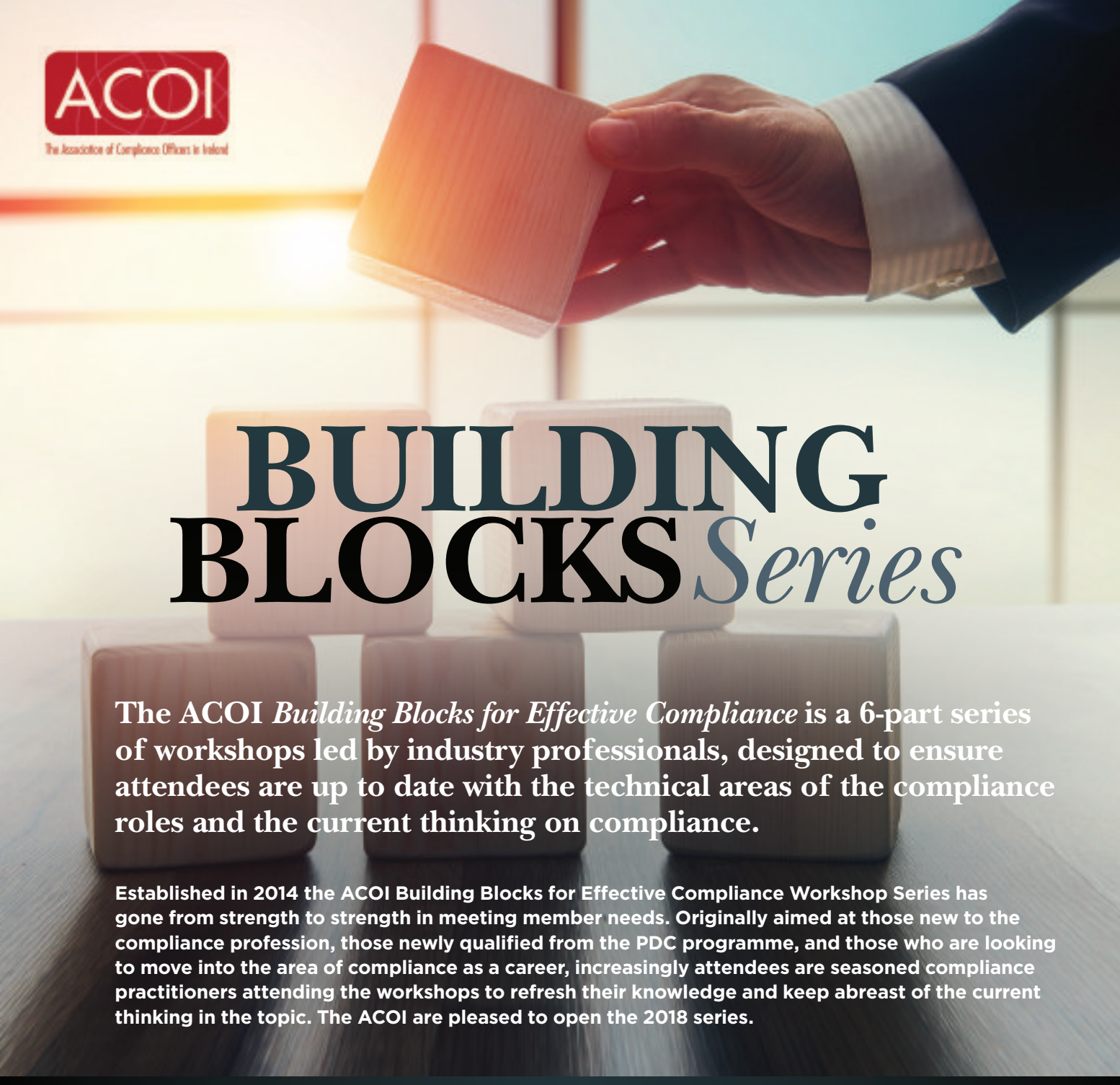
STRONG PRACTICE

- Deploy ABAC specific HR led employee screening practices and track the number and percentage of new and existing employee hires with bribery/corruption negative news, especially for PCF/ CF role holders and other high earners identified by Sales/ Remuneration Committees.

WEAK PRACTICE

- Customer Economic Sanctions/ Counter Terrorist Financing screening practices attributed to ABAC Controls where no employee specific PEP identification and/ or ABAC negative news list screening is deployed. ICQ

Philip Wilson is an ACOI member. He works in abac program management for a multinational bank headquartered in Ireland.



BUILDING BLOCKS *Series*

The ACOI *Building Blocks for Effective Compliance* is a 6-part series of workshops led by industry professionals, designed to ensure attendees are up to date with the technical areas of the compliance roles and the current thinking on compliance.

Established in 2014 the ACOI Building Blocks for Effective Compliance Workshop Series has gone from strength to strength in meeting member needs. Originally aimed at those new to the compliance profession, those newly qualified from the PDC programme, and those who are looking to move into the area of compliance as a career, increasingly attendees are seasoned compliance practitioners attending the workshops to refresh their knowledge and keep abreast of the current thinking in the topic. The ACOI are pleased to open the 2018 series.

11th April:	Regulatory Priorities
9th May:	Role of the Compliance Officer
12th June:	Compliance Plan and Compliance Monitoring
28th August:	Risk Assessment
16th October:	Culture and Conduct
11th December:	Regulatory Risk Monitoring and Compliance Reporting

BOOK ALL SIX EVENTS IN THE SERIES FOR A DISCOUNTED PRICE.*

Members:
- One Event €50
- Six Events €250

Non-Members:
- One Event €75
- Six Events €375

**6 workshops for the price of 5.*

For more information on each event, including venues and speakers, please visit www.acoi.ie/events-calendar

» BOOK HERE

CPD Accredited

ICQ

Data Protection & Technology Working Group

DATA PROTECTION BILL

PUBLISHED – DP&T

Introduction

The Data Protection Bill 2018 was published on 1 February 2018. As the GDPR will come into force in a only a few months, the Oireachtas will need to quickly progress the Bill towards enactment before the 25th of May. **This article is based on the Bill 'as initiated'.**

As expected, the Bill does not represent a major departure from the General Scheme of the Bill published last summer. However, at 128 pages, there is much to digest. This article describes how the Bill shapes up against the GDPR, and how this new regulatory framework will impact compliance officers and practitioners.

Conformity with the GDPR

The Bill implements the GDPR and Directive 2016/680/EC, which concerns the processing of personal data by law enforcement bodies. It will replace the Data Protection Acts 1988 and 2003, save in respect of situations that involve national security, defence and international relations. While the GDPR has direct effect throughout the EU, the Bill is necessary to ensure that the Office of the Data Protection Commissioner (ODPC) has the powers necessary to enforce the GDPR while also ensuring that Ireland clarifies its position in relation to those areas of the GDPR where Member States are required ore permitted to adopt national measures.

Accordingly, the Bill contains certain derogations from the GDPR and other EU-sanctioned enabling measures. The current draft requires extensive cross-referencing to the GDPR itself in order to fully understand what compliance efforts will require. It is also likely that the Bill will, over time, be supplemented by Ministerial regulations that are anticipated in several sections of the Bill. For example, statutory instruments may be adopted to specify "suitable and specific measures" for processing (Section 32(2)), categories of processing that can be carried out in the public interest (sections 34(4) and 45(3)), and instances where data subject rights can be restricted in the public interest (section 54(6)).

Grounds for Processing Personal Data

There is good news for the financial services industry in the form of a provision for the processing of health data where needed for insurance policies, pensions and mortgages (section 44). Section 49 is also useful in permitting the processing of data related to criminal convictions, which will assist with fraud prevention.

In the public sector, controllers will be able to process personal data so that they can perform their prescribed functions (section 34), and section 35 permits processing for purposes other than the reason for which data was collected, where required for national security, public security, preventing, investigating or prosecuting criminal offences, and legal proceedings. Additionally, section 36 affirms that personal data may be processed for archiving, scientific or historical research, or for statistical purposes, where such processing adheres to the principle of data minimisation.

"As expected, the Bill does not represent a major departure from the General Scheme of the Bill published last summer. However, at 128 pages, there is much to digest."

It is also broadly useful that "special" categories of data listed under Article 9 of the GDPR may be processed for the purposes of legal advice, or in relation to legal proceedings (section 41). Additionally, controllers and processors will not be required to register with the DPC, or renew their registrations, after the 25th of May. However, it will remain an offence to process data without the appropriate registration in the interim period.

Restrictions on Data Subjects' Rights

The GDPR enhances the existing suite of data subject rights which are available under the Data Protection Acts 1988 and 2003. The Bill confirms that data subjects will have their GDPR rights to object to automated decision making (section 51) and direct marketing (section 52), and to request the restriction and erasure of processing (section 87). However, restrictions on such rights are outlined in sections 54, 55 and 89. Section 54 in particular will be of far-reaching benefit for private and public controllers, with an interesting new exception for the enforcement of civil claims. Otherwise, many of the restrictions echo those from the existing Data Protection Acts.

Unusually, section 37 facilitates processing for the purpose of

exercising the right to freedom of expression. Unfortunately, there is no guidance as to how organisations should weigh this right against data subject rights. One can expect the law in this area to evolve in the courts.

"Suitable and Specific Measures"

In what appears to be an effort to support data controllers in adopting a "risk based" approach to GDPR compliance (as permitted by Article 24 GDPR), the Bill includes multiple references t o the use of "suitable and specific measures" in the course of data processing. Section 33 provides a non-exhaustive list of "suitable and specific measures," including explicit consent of the data subject, strict time limits for data erasure, training, encryption and other technical and organisational measures. Employers may need to adopt such measures to justify the processing of sensitive data (section 40), as will financial services providers who process health data (section 44).

Some processing will also be permitted subject to the condition that it respects the "essence of data protection", echoing wording from Article 9 GDPR in relation to the processing of special categories of personal data in certain circumstances.

Digital Age of Consent is 13

Section 29 of the Bill confirms that the "digital age of consent" will be 13. Contrary to some media reports, this is only relevant in very specific circumstances where a controller is relying on consent as the lawful basis for providing online services to children. Controllers will remain able to rely on alternative grounds for processing children's data, such as contractual necessity and legitimate interests, where appropriate.

Anticipating Brexit?

Section 34 appears to counteract the impending effects of Brexit by introducing some facilitative provisions for the free movement of data between Ireland and the UK where required to support the common travel area.

"Section 34 appears to counteract the impending effects of Brexit by introducing some facilitative provisions for the free movement of data between Ireland and the UK where required to support the common travel area."

Public Bodies

Contrary to public concerns issued by the ODPC, section 136(3) purports to exempt public bodies from administrative fines, except where they act as an undertaking within the meaning of the Competition Act 2002. This means that public bodies who compete with private bodies may not be exempt from the fines regime so as to avoid distortion of competition where public and private sector bodies compete. The ODPC retains its full suite of other powers and sanctions (including dawn raid powers, rights of audit, information notices, enforcement notices etc) in relation to public and private bodies.

Non-Profit Bodies

Non-profit bodies will be able to assist individuals who seek injunctive and declaratory judicial relief and wish to make complaints to the ODPC. As expected, Bill does not allow such bodies to bring class actions for damages (section 123(7)) which will be a welcome relief for controllers who may suffer a data breach post GDPR commencement.

Powers of the DPC

The new "Data Protection Commission", which will replace the ODPC (section 14), will be empowered to refuse to investigate a complaint, or charge a fee, if the request is manifestly unfounded or excessive (section 96). The Commission will be able to conduct investigations both in response to complaints (section 104), and of its own accord where it suspects that a data protection infringement has occurred (section 105). It will also be empowered to conduct data protection audits (section 131). Generally, the Commission will have more extensive powers to access records, publish reports, appoint expert reviewers, hold oral hearings and publish details of convictions (part 6). It will continue to aim for the "amicable resolution" of all complaints (sections 104 and 107).

There will be a right to appeal the Commission's decisions to the courts within a limited time frame of 28 days. However, even in the absence

of an appeal, administrative fines will be subject to confirmation by the Circuit Court (section 138).

Offences may be punishable by a fine of up to €50,000 or a maximum of 5 years in prison, and will include the unauthorised disclosure of personal data (sections 139 and 140) and enforced access requests (section 4). Where an offence is committed by, or can be attributed to the neglect of a director, manager, secretary or other officer, the Bill includes the standard provision that they may face personal criminal liability (section 141).

Conclusion

The GDPR presents significant challenges for Controllers and Processors which are coming into sharp focus in the countdown to 25 May. Practitioners are also facing an ongoing stream of Article 29 Working Party guidance and any amount of scaremongering within industry and media circles which do not create a supportive environment for those who are trying to adopt a pragmatic and risk based approach to GDPR compliance. While the clarity in the Bill is welcome, it is unfortunate that the Bill has arrived so late in the day, adding another layer of complexity to the legal framework.

At the time of writing the Bill is making its way through the legislative process

and, while there will be little time for many substantive amendments, it is difficult for Controllers and Processors to finalise their GDPR policies and procedures against this moving target. In that context, practitioners are encouraged to focus on the provisions in the Bill governing restrictions on data subjects rights (Sections 54/55) as being perhaps the most significant in the immediate term. ICQ

Rob Corbet, Partner, Head of Technology & Innovation, Arthur Cox, Member of ACOI Data Protection & Technology Working Group *(With thanks to Caoimhe Stafford, trainee in Arthur Cox for her help in preparing this article.)*

'WHAT MAKES FOR AN EFFECTIVE IMPLEMENTATION OF A NEW REGULATION OR PIECE OF LEGISLATION?'

Winner of The Niall Gallagher Professional Diploma in Compliance Scholarship Scholarship - Glenn Cummings. This piece has been authored in the context of implementation of General Data Protection Regulation (GDPR), due for implementation in May 2018, but could be framed for any new regulation.

SECTION ONE

Subject Matter Expertise

Following four years of planning, two years of consultation / interpretation and ninety nine published articles, the sheer depth of expertise and understanding required for effective GDPR implementation may appear daunting, particularly for smaller bodies. Even larger organisations, who may benefit from well- resourced internal compliance teams with multiple subject matters experts in the area of data protection, may find themselves seeking external guidance in the form of legal and business consultancy services. For small organisations and in particular not for profit groups, that challenge is magnified and external guidance may well become the norm, even if it is simply to gain an understanding of potential derogations from GDPR that may apply. That said, there is a delicate balance to be struck between seeking to engineer a robust level of compliance with the regulation and the understanding that GDPR is really designed only to advance and further existing rights, largely already enjoyed to some degree by data subjects across the European Union.

There should, by now, be a firm acknowledgement that firms who have already build a strong data protection foundation and culture across their organisation will have less ground to cover than bodies who may not have invested appropriately to date. Almost daily examples of costly and painful data breaches can be evidenced in the print media in this regard. These firms, in recognizing the reputational damage that they now face following these incidents, must surely redouble their efforts, particularly with GDPR implementation now just a number of months away. The growing industry of data criminality by hacker groups, who seek to harness data protection weaknesses for financial or political gain is ever present. Recent examples of large firms falling victim to these groups must surely demonstrate that better defences are a must. The risk of non- compliance is much more than reputational, with potential financial sanctions of up to €20 million or 4% of turnover for GDPR non- compliance.

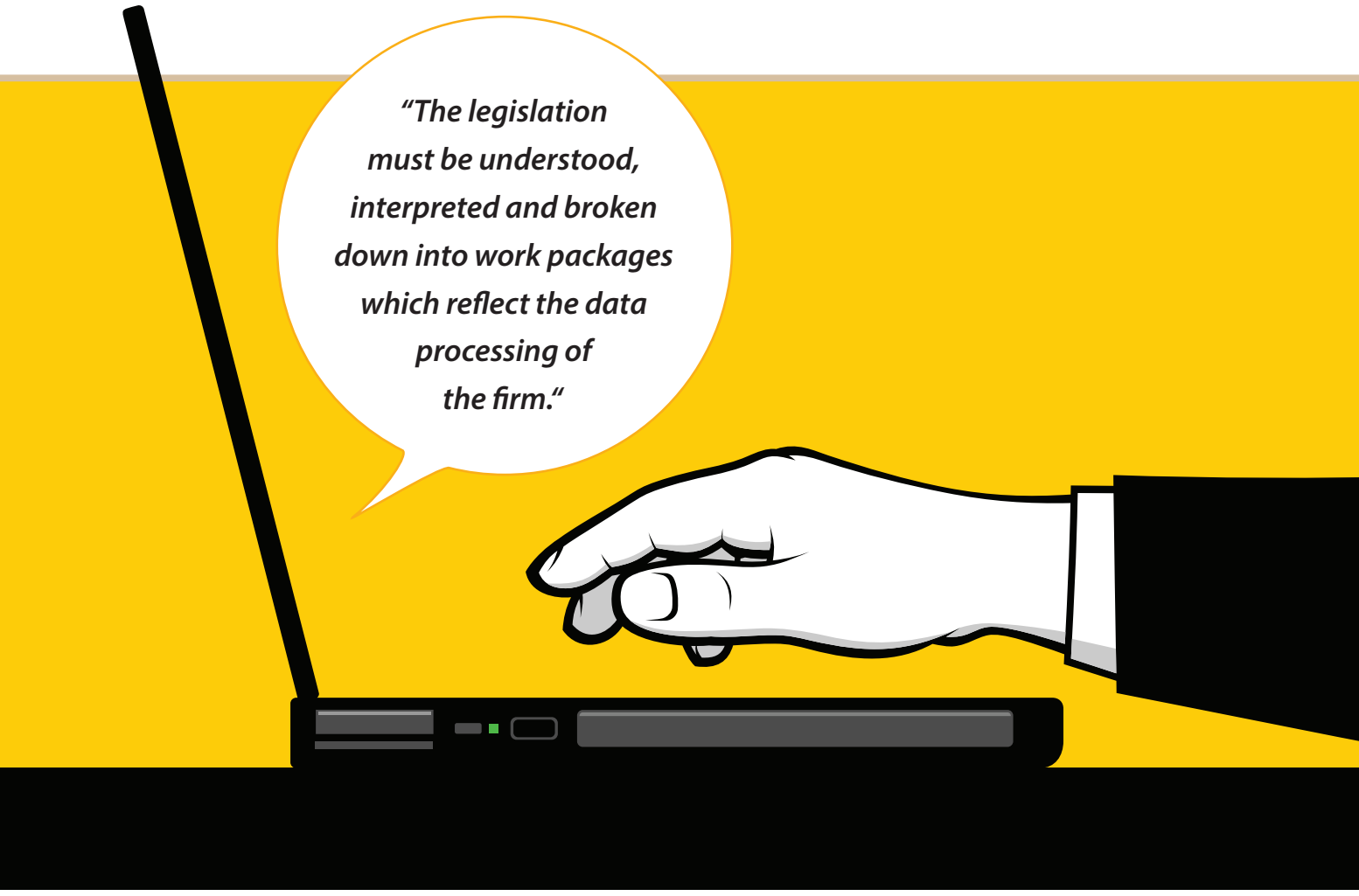
Developing or obtaining subject matter expertise will therefore be a cornerstone of success in the months prior to implementation. The legislation must be understood, interpreted and broken down into work packages which reflect the data processing of the firm.

SECTION TWO

Gap Analysis

Once the expertise has been acquired or made available to the organisation, the next action for implementation will be to identify gaps between current practices and expected processing. While a thorough review of current documented procedures is an obvious place to start in this regard, the scope of this review should also be widened to include practices which may not be fully documented, or practices that have evolved over time and may not reflect the documented procedures they pertain to.

This gap analysis will require expertise and experience from throughout the organisation, in order to fully examine existing practice and culture. While the exercise may appear onerous at first glance, organisations could use this time as an opportunity to gain a clear understanding of their



operations, not only from a data protection viewpoint, but also from a commercial and value standing.

Internally, consideration should be given to the publishing and other socializing of the gap analysis content to the business units which make up the organisation. There may also be value in publishing some of these findings externally, depending on the commercial situation at hand. This exercise should present an opportunity to alter, improve or even halt some data processing that is no longer required. Where faulty (from a GDPR perspective) or no longer required processing is identified in early course, firms should still enjoy ample time to remedy prior to implementation. In the case where remediation timetables are unlikely to be fully delivered prior to implementation date, firms should engage with local regulatory bodies such as the Data Protection Commissioner to communicate their work and plot their route to compliance.

GDPR also mandates a "Data Protection by Design and Default" approach regarding future processing and business design. Firms must get to grips with data protection concerns in early course, particularly when designing new products, services or processes. This intended approach should be documented clearly and used as a foundation for future business change initiatives.

SECTION THREE

The Resources of Remediation

Having analysed existing processing and documented any shortcomings, the next logical phase of implementation is to formulate and execute an appropriate remediation programme.

Bearing in mind the breadth of GDPR, the remediation programme will require a "multi-disciplinary" response – this cannot be seen as merely a compliance project. Particularly in larger organisations, where there may be various layers of processing, primary, secondary and so on - input should be harnessed and resources provided by various business units in order to ensure a cohesive approach. Clear governance in the form of senior stakeholders should be provided, in order to provide authority, direction and purpose. Ultimate accountability for delivery of key objectives will also sit with senior management, with frequent "Red, Amber, Green" reporting as the programme progresses.

In formulating the remediation schedule, due consideration should be given to the likely resourcing requirement in terms of internal expertise, external assistance, and likely I.T spends. These resources should be sized, scheduled and costed, with appropriate budgets and contingencies

SECTION FOUR

Implementation Review

Following delivery of the programme and the implementation date of the measure, a review of the outputs from the programme versus the stated objectives of the remediation plan should be reviewed. Ultimately, the organisation must validate its' own level of comfort in preparation for any second line of defence reviews or inspection by regulatory authorities.

The organisation should also recognise any ongoing efforts for post implementation compliance and ensure that resources remain available to enable these efforts. Any processing that remains non-remediated must now be called out and risk assessed.

Budgets that were prepared for the programme should be reviewed and efforts made to gather any learnings that could be applied to future regulatory change efforts. The time frame for periodic review of data protection architecture should be agreed and documented.

"The benefits of a well thought out and properly executed programme will result in multiple benefits to the organisation and its' customers."

allowed for. It may be useful to review the organisation's risk appetite prior to this scheduling in order to frame the planned remediation response taking into account the organisation's overarching compliance objectives. GDPR legislation allows for the risk analyzing of processing, to allow organisations prioritize their activities based on the level of risk that is present.

Clearly, any processing that is designated as higher risk will be prioritized for remediation prior to GDPR implementation, but Data Protection Officers will need to consult with their executive boards and risk committees to formulate an approach regarding processing that is categorized as mid to low risk. Is it intended, or even possible, to fully remediate these activities prior to implementation or will the organisation's risk appetite permit a phased approach to remediation, which may include post implementation date scheduling – this will be the conversation point.

During this remediation phase, the organisation should also engage with other industry bodies and indeed regulatory authorities to informally peer review their efforts. Any specific industry considerations or efforts may be uncovered and could prove useful to the programme.

The benefits of a well thought out and properly executed programme will result in multiple benefits to the organisation and its' customers. Aside from the obvious advantages of robust compliance and reputational assurance, firms which invest appropriately in data protection measures should also harness competitive advantage by having their data safely secured, correctly accessible and centric to their customer model.

Ultimately, the implementation of this measure will be considered a success if it can stand up to scrutiny, internally and otherwise. Most importantly, the organisation's customers will be the ultimate arbiter in these matters.

As consumers become more concerned with their data – how it is collected, processed, maintained, secured and disposed of, they will ultimately chose organisations with a strong data culture and reputation as their provider of choice. ICQ

Glenn Cummings, ACOI Member.

WHEN FAILURE IS NOT AN OPTION

The challenge of implementing Australian financial services regulation in organisations.

Abstract

This article explores the reasons why implementing Australian Financial Services regulations in organisations is such a challenge. These challenges are important to explore, because such regulations must be implemented successfully if organisations want to continue in business. Many organisations, however, report experiencing mixed levels of success, despite spending significant time and resources on regulatory projects and compliance activities. Using a change management lens, a complex set of interconnected dynamics for regulations and organisations was identified. While many of these underlying forces were found to be in common with other types of large-scale change, a number of critical aspects, unique to implementing regulations, were high-lighted. Of particular note was the emergent nature of regulations, and that success or failure are found to be graduated and partially overlapping bands of activity, rather than precise definitions, with ambiguity particularly at more minimal levels of compliance. To address these challenges, it is suggested in this article that organisations adopt a differentiated approach to managing regulations, depending on the stage in that regulation's lifecycle. Implementation projects could also be planned over a longer timeframe to accommodate the evolution of such regulations, with assessments of the success of these programs ongoing. In addition, awareness of how these unique dynamics operate can assist compliance professionals in arguing for tailored approaches to implementing regulations for their organisation, and to support the business in achieving improved levels of success.

Introduction

For organisations operating in the Australian Financial Service (AFS) industry, failure to implement new or revised AFS regulations is not an option – even if this implementation requires significant business transformation. Organisations must implement compliance changes, and maintain regulatory operations successfully, if they want to continue in business and avoid negative consequences such as legal and financial penalties or reputational damage *(Thomson Reuters 2012)*. This requirement is concerning when organisations frequently experience a mixed level of success, despite spending significant time and financial resources on regulatory projects and compliance activities *(Regulation Taskforce 2006; Productivity Commission 2011)*. The question is: Why is the implementation of AFS regulations such a challenge?

Through a change-management lens, this question is considered from an organisation-centric focus that has received less attention in the literature compared to the legal, policy, design, and regulator activities in financial services *(See Black et al., 2005; Parker and Nielson, 2006; O'Brien, 2010)*. For the purposes of this article, the term regulation refers to AFS regulations and implementation is used to also refer to maintaining the operations of regulations. First, an overview of the challenges facing organisations when implementing regulations is provided by considering

the key characteristics of regulations and organisations. Then, the complex issue of defining success and failure in this context is explored. Using these insights, the implications for increasing the level of success of implementation of regulations in organisations are discussed.

Key characteristics of regulations

The type of regulations being considered within this article are those that are mandatory and imposed by the Australian Federal Government. Examples of such regulations include those required for compliance with the National Consumer Credit Protection reform (NCCP), which commenced in 2010 *(Australian Securities and Investment Commission (ASIC) 2011a)*. While industry lobbying can result in aspects of regulations being clarified or delayed, regulations are typically run to a timetable set by the Government. Regulations can also intrude into an organisation's operating model, requiring significant transformation to business practices, thus impacting upon products, processes, technology and skills. It can also include the structure and culture of an organisation. Such changes are both costly and time-consuming, potentially impacting on relationships with customers, the wider economy and other industries *(Hackman 2006; Baldwin et al. 2012)*. This intrusiveness has increased over the last decade, with regulatory agencies looking for 'genuine compliance' *(Coyle 2012; Thomson Reuters 2012)*. This means organisations are expected to undertake more than minimal compliance, a task made more difficult with the increased amount of regulation, particularly post the 2008 Global Financial Crisis (GFC) *(PricewaterhouseCoopers (PwC) 2011; Accenture 2012; Australian Prudential Regulation Authority (APRA) 2012a)*.

However, these regulations are not necessarily rigid and prescribed because the new laws that underpin regulations are untested. Additionally, they can be interpreted in a number of different ways, and do not cover all situations. Amendments can be made to clarify the laws and refine regulations. Often, such amendments are based on feedback from industry, meaning that regulations are emergent with design and implementation running in parallel *(Black 2002; Hackman 2007)*. Amendments can continue after regulations come into effect, particularly if they do not deliver intended benefits, or result in unintended consequences *(Bookstaber 2007)*. Adding to the emergent nature of regulations is an inherent ambiguity in their operation. Rules-based regulations cannot cover every situation that can occur; principle-based regulations are open to interpretation; and methods for assessing effective implementation can evolve over time *(Downer 2008; Mullins 2008; O'Brien 2010; Coyle 2012)*. This means that organisations have a level of discretion when deciding how they will interpret the rules, or principles, in order to make them work for their organisation *(Hofmann 2008)*.

Furthermore, regulations are managed by a number of different regulatory agencies *(Department of Finance and Deregulation 2012)*. This means organisations may have to deal with a range of regulatory agencies, all of which require different types of responses and processes to implement regulations. Given this complexity, regulations do not have a track record of being easy to implement, often resulting in higher costs and requiring subsequent remediation projects *(Regulation Taskforce 2006; Productivity Commission 2010)*. Yet, the Government depends on organisations, as its agents, to implement regulations successfully for the intent of the reform to be delivered.

Key characteristics of organisations

While the types and sizes of organisation required to implement regulations are varied, there are some common characteristics that can be considered for this discussion. For instance, the amount and pace of change for these organisations has increased exponentially in recent years, due to pressures from changing markets, new technology requiring nimble business responses and a greater amount of both AFS specific and more general business regulation to implement *(Morgan & Page 2008; Drezensky et al. 2012; Tandulwadikar 2012)*. As a result, there is competition for change resources within organisations. In the current climate, few change resources are being diverted to regulatory implementation activities *(PwC 2011)*.

However, even when resources are made available, it is not simple to undertake these regulatory implementation activities. Such projects require large-scale change programs, involving a range of internal stakeholders *(Kotter & Cohen 2002; Hackman 2005; Palmer et al. 2006; McFillen et al. 2012)*. Resistance from stakeholders, usual in all change, is amplified when implementing regulations *(Hackman, 1999; Mento et al., 2002; Atkinson, 2005; van Dijk, 2009)*. The emergent nature of regulations typically creates frustrations, as plans must change, often increasing costs and reducing productivity. The mandatory nature and low confidence intended benefits will be delivered often increases this resistance. Nor can agreement necessarily be reached as to how the implementation should be approached *(Weick & Quinn 1999; Bolman & Deal 2008; Nasim & Sushil 2011)*. Instead, there can be a range of different perspectives from internal stakeholders about which issues are most important and what comprises success.

"Regulations can intrude into an organisation's operating model, requiring significant transformation to business practices, thus impacting upon products, processes, technology and skills."

For instance, the CEO may regard corporate reputation issues as most important, while the business or line manager may be more concerned about keeping the business running smoothly. Frontline employees, who may be change-weary, just want to know what to do. Similarly, other areas of the business will have their perspective and particular concerns. These different perspectives can be positive, because they prompt conversations about new ways of organising and indicate that people are not disengaged *(McClellan 2011; Piderit 2000)*. However, they can also lead to unpopular compromises and trade-offs. Despite these challenging dynamics, organisations do engage and implement regulations, even though their methods may vary.

Recent research investigating the implementation of new and revised regulations found that organisations do vary in their typical approach from a more minimalistic, reactive response, to a more comprehensive proactive response, reflecting the level of activity undertaken *(Hackman 2009a, 2009b)*. One key finding in a report undertaken on the AFS industry was that an organisation's level of success with previous regulatory implementations was the major influence on that organisation's response. Thus, if the previous implementation was more successful, the organisation will be subsequently more proactive and do more when next implementing regulations. Conversely, if the previous implementation was less successful, then the organisation will be more reactive and do less when next implementing regulations. The implication for organisations reporting a mixed level of success is that they may decrease their efforts to be proactive when implementing regulations because of these experiences.

These findings are consistent with change literature regarding the impact of poor change experiences and the influence of leaders and managers in encouraging certain behaviours in change implementation *(Pettigrew et al. 2001; Bordia et al. 2011; Dalton 2007; Uhl-Ben et al. 2007)*. In this context, poor change experiences become part of an organisation's memory, prompting resistance to subsequent regulatory change initiatives. These findings also link the impact of positive experiences to creating readiness for change, and to where leaders and managers can support the adoption of positive attitudes into the culture and influence 'the way things are done around here' *(Armenakis et al. 2002; Armenakis & Harris 2009)*. The result is that people are more ready to engage with subsequent regulatory change initiatives. Therefore, reactions to implementing regulations, whether positive or negative, contribute to creating an organisation's compliance culture.

Why implementing regulations is such a challenge

These key challenges for implementing regulations in organisations are summarised in Figure 1 and highlight the competing pressures, complexity and resource-hungry nature of these types of change initiatives.

But are these challenges, in this regulatory context, so unique? Many are shared by other types of large-scale change initiatives. For example, during the 1990s, publishers globally had to move to digital publishing models in order to continue operating in the industry *(Martin & Tian 2010)*. There was competition for scarce change resources, as these technological changes were implemented while organisations also continued business-as-usual activities and other business development projects. These changes intruded into the functioning of many organisations, as well as impacting on the delivery of products and services, and customer relationships. This required many compromises, with many different points of view needing to be reconciled. Due to the untested nature of these technological changes, there was ambiguity about what to implement, requiring costly revisions as organisations sought to achieve their desired outcomes. These complex and resource-hungry changes have continued, with newspapers now required to be available in many digital, as well as paper, formats *(INSEAD 2007; Wharton School of the University of Pennsylvania 2013)*.

However, despite similarities, there are unique aspects that make the implementation of regulations even more challenging. The Government imposes regulations on organisations, which also captures customers who are required to use the new products or services. The Government has the ability to penalise organisations, if they fail to achieve appropriate implementation. However, the Government also relies on organisations, as their agents, to implement regulations successfully for the intent to be achieved – a situation made more difficult because what organisations need to achieve is emergent, open to interpretation and often revised. There is a multiplier effect, with organisations required to implement a greater amount of regulations, post-GFC, at different stages of development. involving a number of different regulatory agencies. This means organisations are not just dealing with one change initiative, but must consider what they can do to improve their success rate across a regulatory portfolio comprising multiple change initiatives. As a result of the unique challenges in this context, organisations face the difficulty of defining the success that, on the one hand, they want to achieve and, on the other hand, must achieve for an increasingly complex range of regulations.

The difficulty of defining success (and failure)

Organisations do choose different levels of activity when implementing regulations. This can range from the minimum compliance, generally more focussed on keeping costs down, through to a more comprehensive approach to, for instance, creating a competitive advantage through compliance, or benefits for customers. This range of responses means that, from the organisation's perspective, there can be different definitions of success, depending on the situation. To do the minimum to comply with a regulation, for one organisation, could be considered success. For another, aiming for a more comprehensive approach, achieving only the minimum level could be considered a failure. There can also be a temporal aspect to success, depending on what organisations want to achieve. With the increase in regulation post-GFC, near enough, or almost complying, may be considered a successful outcome, particularly if requirements are unclear. Typically, this level of activity would be a first step, with the intention to undertake additional implementation activities later, when operation of regulations is more established. Therefore, organisations choose the level of success they want to achieve; however, the definition may differ across organisations. But how does this variable response reconcile with what organisations must achieve?

> ***"Regulatory agencies have indicated expectations for genuine compliance that entails doing more than the minimum, or only technical compliance."***

Regulatory agencies have indicated expectations for genuine compliance that entails doing more than the minimum, or only technical compliance. It could, therefore, be concluded they would consider success means doing more than just complying with laws and regulations, and that anything less would be considered failure. However, a review of regulatory requirements indicates there may be situations, when this would not be the case, and partial success may be acceptable. For instance, regulatory agencies can use transitional arrangements for regulations, creating

a staged approach to implementation *(ASIC 2011b)*. Partial compliance may also be acceptable, when there are new requirements and they want to take a more facilitative role, the design of regulations makes implementation difficult, or when the regulation is not working as expected *(Lynch 2013)*. This reflects the reality that organisations can only do as well with regards to implementation as the design of the regulations allows, and that regulators can only provide guidance to the extent the law and associated regulations are clear in their operation. However, more can also be expected, because the minimum level for compliance can increase as the operations of the regulations are clarified.

Assessments of success can also differ between types of regulations managed by different regulatory agencies *(APRA 2012b)*. Some can be more behavioural-focussed, concerned with black letter law, rules and penalties, while other can be more outcome or risk-based-focussed, concerned with principles and prevention. The tolerance for partial or staged success is likely to be lower for behavioural regulations, but higher for risk-based regulations. However, particularly if regulations have been in operation for some time, regulatory agencies may assess any actions that do not meet genuine compliance requirements as failure. This can occur if, in their view, the intended outcomes are being undermined by the organisation's actions. Assessment of failure would also occur if laws and regulations are broken, due to wilful or criminal non-compliance *(ASIC 2012; Kehoe & Thompson 2013)*. Therefore, defining the success that must be achieved depends on how the regulatory agencies assess the organisation's effort and intentions, the development stage and type of regulation and whether the regulations are work appropriately in the view of the regulatory agencies.

As illustrated in Figure 2, combining the different views about what organisations want and need to achieve shows that success and failure are graduated and partially-overlapping bands of activity, rather than precise definitions. Two additional categories of below-minimum compliance are used, in addition to the levels of implementation activity suggested by Hackman *(2009a, 2009b)*. On this expanded continuum, failure can range from Not Comply, through Partially Comply, to Comply, with the upper level reflecting the view of regulatory agencies that organisations should do more than the minimum. Success can range from Partially Comply, reflecting achievement of some success from either the organisation or regulatory agency view, with increasing levels of success when more activities are undertaken, through Do More to Do Extra. Any response below Partially Comply would be failure and above Comply would be success. However, in between these levels, there is an Overlapping Zone comprising Partially Comply and Comply, where assessments can be success or failure, depending on a range of factors, some of which might lie outside the organisation's control.

Discussion

Given the dynamics involved in defining success and failure, it is not surprising organisations report experiencing mixed levels of success. There are many moving parts to consider, with three aspects of particular importance. Firstly, there is a level of ambiguity, with potentially subjective assessments of whether actions constitute success or failure at the more minimal levels of compliance. Secondly, as regulations mature in operation, the minimum level for compliance can increase. This means that what was the minimum previously can become partial compliance and potentially assessed as failure, rather than success. This shift in goal posts for minimum compliance can occur more than once during the lifetime of a regulation. Thirdly, organisations can, to an extent, choose what they consider to be success – dependent, for instance, on their operations, culture and aspirations.

The implication and interaction of these moving parts is that it may not be possible to have meaningful comparisons of success across organisations, except when compliance actions are defined clearly. This is unlikely to be satisfactory to organisations and regulators, when

the focus for success is not only on implementing regulations, but also on achieving the intent of the regulations *(Australasian Compliance Institute (ACI) 2009; APRA 2012b)*. Of concern, when considering Hackman's *(2009a, 2009b)* recent research, is evidence supporting the fact that organisations need to experience success before becoming more proactive in their next regulatory implementation. No doubt organisations do want to comply by implementing regulations appropriately, but continuing to experience mixed levels of success may reduce their enthusiasm, as well as make it harder for compliance professionals to argue for resources and to implement more than a reactive response. The danger here is that such responses may fall into the Overlapping Zone, where there is ambiguity about the definitions for success and failure, thereby perpetuating, rather than improving, the current mixed experiences.

So is there anything organisations can do to improve their levels of success? One approach, based on the discussion of success and failure, could be to do more than the minimum to comply, for all regulations. This would raise the level of implementation for all regulations and avoid any ambiguity about the outcome. The disadvantage with this approach is that it could actually lead to lower levels of success because regulations differ not only in their duration and the complexity of change activities required, but also their operational maturity *(Murray 2007; Hackman 2008; Mullins 2008)*. Higher levels of compliance activity may suit some more complex and operationally-mature regulations, but may not suit others, particularly when requirements are still emerging, or being revised. So would it be better to do only the minimum for all regulations? Again, this approach may suit some regulations, but not others. Instead, differential effort across regulations, commensurate with their clarity of requirements and maturity, is likely to result in better use of resources and higher levels of success than using a one-size-fits-all or standardised approach.

"To accommodate the changing requirements as regulations mature, organisations could also plan regulatory projects to continue over a longer period."

To accommodate the changing requirements as regulations mature, organisations could also plan regulatory projects to continue over a longer period, supported by appropriate change implementation activities *(Hackman 2008)*. Current practice, particularly in larger organisations, tends to focus on instigating regulatory projects that conclude once a go-live date is achieved, with regulatory activities and subsequent changes handed to the business to manage. The mixed rates of success experienced by organisations could stem from assessments being made at this point, when it is unlikely that all aspects of regulatory operations have been clarified, or could be implemented effectively. Instead, success could be assessed progressively, as stages of the implementation are completed over a longer timeframe, reflecting a more realistic approach to measuring outcomes.

While these two suggestions could assist with improving the level of success, it is also clear, from the discussion of the dynamics impacting the implementation of regulations, that there is no one right way to suit all situations. The need will always exist to take into account the history, complexity and the particular focus of the organisation's operations, in order to select the appropriate approach. Nevertheless, the insights presented in this discussion, particularly about the unique dynamic involved in assessments of success and failure, can assist compliance professionals to support the business to develop more targeted plans, the implementation of regulations and more appropriate allocation of resources over time, to achieve success appropriate to the organisation.

Conclusion

This article explored some of the many reasons why implementation of regulations in organisations is such a challenge. The concern is that organisations often report experiencing a mixed level of success, despite spending significant time and financial resources on regulatory projects and compliance activities. So what can organisations do differently? Using a change management lens, this article highlighted the unique dynamics involved with implementation of regulations, particularly their emergent nature and potential variations in definitions for success and failure. Two suggestions are offered to assist with improving success: use of a differentiated approach to manage regulations and implementation projects planned over a longer timeframe, to accommodate the evolution of regulations. In addition, awareness of how these unique dynamics operate can assist compliance professionals to argue for tailored approaches to implementing regulations for their organisation and to support the business in achieving improved levels of success. ICQ

REFERENCES

Accenture 2012, The Challenge of Regulatory Implementation: A Strategic Approach, Available at http://www.accenture.com/SiteCollectionDocuments/PDF/Accenture-Challenge-Regulatory-Implementation.pdf (accessed 18 September 2012).

Armenakis, AA & Harris, SG 2002, 'Crafting a change message to create transformational readiness', Journal of Organizational Change Management, vol. 15, no 2, pp. 169-183.

Armenakis, AA & Harris, SG 2009, 'Reflecting: our journey in organizational change research and practice', Journal of Change Management, vol. 9, no. 2, pp. 127-142.

Atkinson, P 2005, 'Managing resistance to change,' Management Services, vol. 49, no. 1, pp. 14-17.

Australasian Compliance Institute (ACI) 2009, Financial Services Regulator Panel discussion, Australasian Compliance Institute's 2009 annual conference, Sydney.

Australian Bureau of Statistics (ABS) 2012, Counts of Australian Businesses, including Entries and Exits, Jun 2007 to Jun 2011, cat. no. 8165.0, issued 31 January 2012. Available at

http://www.abs.gov.au/AUSSTATS/abs@.nsf/DetailsPage/8165.0Jun%202007%20to%20Jun%202011?OpenDocument (accessed 1 October 2012).

Australian Prudential Regulation Authority (APRA) 2012a, Bank Regulation and the Future of Banking, Presented by J.F. Laker to 41st Australian Conference of Economists, Melbourne, 11 July. Available at http://www.apra.gov.au/Speeches/Documents/John%20Laker%27s%20%20Australian%20Economic%20Forum%2011%20July%202012.pdf (accessed 14 October 2012).

Australian Prudential Regulation Authority (APRA) 2012b, Australian Prudential Reform: Where are we now, and where are we going?, Presented by C. Littrell to the Chief Risk Officers Forum 2012 Conference, Sydney, 26 September. Available at http://www.apra.gov.au/Speeches/Pages/Australian-prudential-reform-where-are-we-now-and-where-are-we-going.aspx (accessed 14 October 2012).

Australian Securities and Investment Commission (ASIC) 2011a, Credit Licensing: Responsible Lending Conduct, Regulatory Guide 209. Available at http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/rg209-310311.pdf/$file/rg209-310311.pdf (accessed 19 July 2012).

Australian Securities and Investment Commission (ASIC) 2011b, Credit Disclosure: Transitional arrangements. Available at http://www.asic.gov.au/asic/ASIC.NSF/byHeadline/Credit-disclosure-INFO-137 (accessed 19 October 2012)

Australian Securities and Investment Commission (ASIC) 2012, Media release: 12-237MR Former mortgage broker pleads guilty to first charges laid under the National Credit Act. Available at http://www.asic.gov.au/asic/asic.nsf/byHeadline/12-237MR%20Former%20mortgage%20broker%20pleads%20guilty%20to%20first%20charges%20laid%20under%20the%20National%20Credit%20Act?opendocument# (accessed 27 September 2012).

Baldwin, R, Cave, M & Lodge, M 2012, Understanding Regulation Theory, Strategy and Practice, 2nd edn, Oxford University Press, New York, NY.

Black, J 2002, 'Critical reflections on regulation', Australian Journal of Legal Philosophy, vol. 27, pp. 1-36.

Black, J, Lodge, M & Thatcher, M 2005, Regulatory Innovation: A comparative analysis, Edward Elgar, Cheltenham, UK.

Bolman, LG & Deal, TE 2008, Reframing Organizations, 4th edn, Jossey Bass, San Francisco, CA.

Bookstaber, R 2007, Demon of our own Design, John Wiley & Sons, Ltd, Hoboken, NJ.

Bordia, P, Restubog, SLD, Jimmieson, NL & Irmer, BE 2011, 'Haunted by the past: effects of poor change management history on employee attitudes and turnover', Group & Organization Management, vol. 36, no. 2, pp. 191-222.

Coyle, M 2012, Financial Action Task Force (FATF) reveals plans to assess 'effectiveness' as well as technical compliance, Complinet 15 October. Available at http://www.complinet.com/global/news/news/article.html?ref=159229&bulletin=spotlight&region=_217220 (accessed 15 October).

Dalton, M 2007, 'An investigation into the impact of national culture on a compliance culture', Compliance and Regulatory Journal, vol. 2, pp. 45–57.

Department of Finance and Deregulation 2012, Financial Regulation. Available at http://australia.gov.au/topics/economy-money-and-tax/financial-regulation (accessed 15 October 2012)

Downer, J 2008, 'What finance could learn from rocket science', Risk & Regulation, Financial Crisis Special, p. 19.

Drzensky, D, Egold, N & van Dick, R 2012, 'Ready for a change? A longitudinal study of antecedents, consequences and contingencies of readiness for change', Journal of Change Management, vol. 12, no. 1, pp. 95-111.

Hackman, K 1999, 'Understanding and managing resistance to change', HR Monthly, April, pp. 8-9.

Hackman, K 2005, 'Providing customers with the 'right help': Implementing the financial services reform in Insurance Australia Group', Journal of Change Management, vol. 5, no. 3, pp. 345-355.

Hackman, K 2006, 'Using the service encounter to facilitate regulatory change', Strategic Change, vol. 15, no. 3, pp.145-152.

Hackman, K, 2007, 'Beyond administrations: Redefining the challenge for regulatory change', Strategic Change, vol. 16, no. 1-2, pp.1-9.

Hackman, K 2008, 'Fit for purpose: Strategies for effective implementation of regulations', Compliance & Regulatory Journal, vol. 5, pp. 33-38. Also available at http://khassociates.com.au/publishing.html (accessed 18 August 2012).

Hackman, K 2009a, Regulation View 2009 Benchmark Report about Implementation of Regulations in Organisations, UTS Scholarly Works Collection. Available at http://hdl.handle.net/2100/1068 (accessed 15 July 2012).

Hackman, K 2009b, 'Encouraging organisations to do more than just comply with regulations', Compliance & Regulatory Journal, vol. 7, pp. 28-38. Also available at http://khassociates.com.au/publishing.html (accessed 18 August 2012).

Hofmann, J 2008, 'Cyclic dreams of a strong state', Risk & Regulation, Financ ial Crisis Special, p 9.

Innovation & Business Skills Australia (IBSA) 2012, Environment Scan – 2012: Financial Services Industry (Innovation & Business Skills Australia). Available at http://www.ibsa.org.au/Portals/ibsa.org.au/docs/Research%20&%20Discussion%20Papers/Escan/EScan2012/IBSA%20Escan%202012%20-%20Financial%20Services.pdf (accessed 1 October 2012).

INSEAD. (2007) New Media: The online evolution of newspapers. INSEAD Knowledge. Available at http://knowledge.insead.edu/leadership-management/strategy/new-media-the-online-evolution-of-newspapers-1965?vid=14 (accessed 4 October 2012).

Kehoe, J & Thompson, S 2013, 'The mess Macquarie made', Australian Financial Review, 16-17 February, pp. 14-15.

Kotter, JP & Cohen, D 2002, The Heart of Change, Harvard Business School Press, Boston, MA.

Lynch, N 2013, 'ASIC signals 'facilitative' approach to compliance as FoFA deadline looms'. Complinet, Thomson Reuters, Feburary 18. Available at http://www.complinet.com/global/news/news/article.html?ref=162138&bulletin=spotlight&region=_217220 (accessed 18 February 2013)

McClellan, JG 2011, 'Reconsidering communication and the discursive politics of organizational change', Journal of Change Management, vol. 11, no. 4, pp. 465-480.

McFillen, JM, Deborah, A, O'Neil, DA, Balzer, WK & Varney, GH 2012, 'Organizational diagnosis: An evidence-based approach', Journal of Change Management, DOI:

10.1080/14697017.2012.679290, Version of record first published: 18 Jun 2012.

Martin, B & Tian, X 2010, Books, Bytes and Business: The Promise of Digital Publishing, Ashgate Publishing Group, Farnham, Surrey.

Mento, AJ, Jones, RM & Dirndorfer, W 2002, 'A change management process: Grounded in both theory and practice', Journal of Change Management, vol. 3, no. 1, pp. 45-59.

Morgan, RE & Page, K 2008 'Managing business transformation to deliver strategic agility', Strategic Change, vol. 17, pp. 155-168.

Murray, JW 2007, 'How has the practice of compliance management evolved and what are the key lessons learned? How can this be used as a model to improve the future?' Compliance and Regulatory Journal, vol. 2, pp. 24–38.

Mullins, G 2008, 'Prescriptions and principle: The implications of different regulatory models for compliance professionals', Compliance & Regulatory Journal, vol. 4, pp. 32-38.

Nasim, S & Sushil 2011 'Revisiting organizational change: Exploring the paradox of managing continuity and change', Journal of Change Management, vol. 11, no. 2, pp.185-206.

O'Brien, J 2010, 'The future of financial regulation: Enhancing integrity though design'. Sydney Law Review, vol. 32, pp. 63-85.

Palmer, I, Dunford, R & Akin, G 2006, Managing Organizational Change, Hill/Irwin, New York.

Parker, CE & Nielson, VL 2006, 'Do businesses take compliance seriously? An empirical study of the implementation of trade practices compliance systems in Australia', Melbourne University Law Review, vol. 30, pp. 441-494.

Piderit, S.K. (2000) Rethinking resistance and recognizing ambivalence: A multidimensional view of attitude toward an organizational change, Academy of Management Review, 25(4), pp.783-794.

Pettigrew, AM, Woodman, RW & Cameron, KS 2001, ' Studying organizational change and development: Challenges for future research', Academy of Management Journal, vol. 44, no. 4, pp. 697-713.

Productivity Commission 2010, Annual Review of Regulatory Burdens on Business: Business and Consumer Services, Research Report, Productivity Commission, Canberra, Australia.

Productivity Commission 2011, Identifying and Evaluating Regulation Reforms, Research Report, Productivity Commission, Canberra, Australia.

PricewaterhouseCoopers (PwC) 2011, 'What does regulatory change mean for your business?' PwC Regulatory Change Benchmarking Survey, July 2011. Available at http://www.pwc.com.au/industry/banking-capital-markets/assets/Regulatory-Change-Benchmarking-Survey-2011.pd (accessed 18 August 2012).

Regulation Taskforce 2006, Rethinking Regulation: Report of the Taskforce on Reducing Regulatory Burdens on Business, Canberra, Australia: Commonwealth of Australia.

Tandulwadikar, A 2012, 'Innovation Imperatives in retail banking', Cognizant Reports, August 2012. Available at http://www.cognizant.com/InsightsWhitepapers/Innovation-Imperatives-in-Retail-Banking.pdf (accessed 20 September 2012).

Thomson Reuters 2012 Special Report: Global Trends in Enforcement of Financial Services Regulations. Available at http://thomsonreuters.com/content/news_ideas/articles/financial/693411 (accessed 24 July 2012).

Uhl-Ben, M, Marion, R & McKelvery, B 2007, 'Complexity leadership theory: Shifting leadership from the industrial age to the knowledge era', The Leadership Quarterly, vol. 18, pp. 298-318.

van Dijk, R & van Dick, R 2009, 'Navigating organizational change: Change leaders, employee resistance and work-based identities', Journal of Change Management, vol. 9, no. 2, pp. 143-163.

Weick, KE & Quinn, RE 1999, 'Organization change and development', Annual Review of Psychology, vol. 50, pp. 361-386.

Wharton School of the University of Pennsylvania 2013, 'Journalism in the Digital Crossfire: Who Will Pay for the News?': Knowledge@Australian School of Business, February 19. Available at http://knowledge.asb.unswedu.au/article.cfm?articleid=1756 (accessed 21 February 2013).

Regulation & Compliance

Domestic

- Minimum Competency Code 2017 and Minimum Competency Regulations 2017 - Questions and Answers
- Data Protection Bill 2018
- Response to the Committee on Public Petitions in response to correspondence on Petition No P00047/17
- Guidance for Completion of the Anti-Money Laundering, Countering the Financing of Terrorism and Financial Sanctions: Risk Evaluation Questionnaire
- Competition and Consumer Protection (Amendment) Bill 2018
- Companies (Statutory Audits) Bill 2017
- Consumer Protection (Regulation of Credit Servicing Firms) (Amendment) Bill 2018
- Markets Update Issue 3 2018
- Markets Update Issue 4 2018
- Research Bulletin No.10
- Financial Globalisation and Central Banking in Ireland - Governor Philip R Lane
- We continue to challenge the effectiveness of the underlying culture in banks - Director General Derville Rowland.

European

- Consultation on the review of the SME definition
- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 575/2013
- Commission Delegated Regulation (EU) 2018/171
- Composition of the Working Group on Euro Risk-free Rates Announced
- ESMA publishes 2018 Supervisory Convergence Work Programme
- ESMA publishes 2018 work programme for CRAs, trade repositories and third country CCPs
- ESMA publishes risk assessment work programme for 2018
- EBA publishes corrective update of XBRL taxonomy 2.6 for remittance of 2018 benchmarking exercise
- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 575/2013
- Proposal for a Directive of the European Parliament and of the Council amending Directive 2014/59/EU
- Proposal for a Directive of the European Parliament and of the Council amending Directive 2013/36/EU
- Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 806/2014
- Article 29 Working Party - February 2018 Plenary Meeting
- Keynote Address: A Measured Approach to Fintech
- Commission Implementing Regulation (EU) 2018/292
- Draft Withdrawal Agreement published by European Commission
- Reaping the benefits of payment services in a new regulatory environment
- Statement by Danièle Nouy, chair of the Supervisory Board of the ECB
- ESAs warn consumers of risks in buying virtual currencies

Funds

Domestic

- Improvements to Central Bank rules for Loan Originating Qualifying Investor AIFs
- Benchmarks Regulation – Updated ESMA Q&As

European

- EU Commission notices on the consequences of Brexit on Asset Management
- MMF Regulation - EU Commission letter to ESMA on share cancellation
- CIS liquidity risk management - IOSCO recommendations and good practices
- ESRB recommends that ESMA and the EU Commission develop legislation and guidance on leverage and liquidity in investment funds
- ESMA interactive single rulebook
- EU Commission survey on the functioning of the AIFMD

Banking

Domestic

- Research on the impact of repossession risk on mortgage default

European

- Introductory statements at the annual press conference on ECB Banking Supervision
- EBA updates its methodological guide on risk indicators and detailed risk analysis tools
- ECB amends guidelines relating to the Eurosystem's monetary policy implementation
- Research bulletin no. 43: Bank lending under negative policy rates
- ECB publishes consolidated banking data for end-September 2017
- EBA issues Opinion on measures to address macroprudential risk
- Cross-border banking in the EU since the crisis: what is driving the great retrenchment?

Investment

Domestic

- Reporting requirements for MiFID investment firms

European

- ESMA updates Q&A on EMIR implementation
- ESMA updates Q&As on the Benchmarks Regulation
- ESMA updates its CSDR Q&As
- ESMA issues conflict of interest guidelines for CCPs
- ESMA updates its MiFID II Q&As on transparency and market structures
- ESMA updates its Q&A on short selling
- ESMA Technical Advice on the evaluation of certain elements of the Short Selling Regulation (SSR) of 21 December 2017
- EU Commission notices on the consequences of Brexit on Asset Management
- ESMA interactive single rulebook

Insurance

Domestic

- Central bank director of insurance supervision speech on governance and role of independent directors
- Cost of insurance working group publishes fourth update on progress
- Department of finance consults on national claims information database

European

- Council of EU confirms IDD delay
- EIOPA issues second set of advice on amendments to the Solvency Capital Requirement
- EIOPA publishes paper on systemic risk and macroprudential policy in the insurance sector
- Insurance Europe publishes Brexit position papers
- Insurance Europe responds to EIOPA call for input on reporting and disclosure
- European Parliament publishes resolution on EU/USA Bilateral Agreement on prudential measures regarding insurance and reinsurance
- European Commission publishes notice on the impact of Brexit on EU (re)insurance rules
- EIOPA publishes Solvency II statistics
- EIOPA Decision on annual market and credit risk modelling comparative study
- Insurance Europe publishes annual insurance data
- EIOPA Chair Speech on the Review of Solvency II
- Solvency II Implementing Regulation – calculation of technical provisions & basic own funds. ICQ

MEMBER Profile

Brendan McWeeney

Brendan McWeeney,
Head of Compliance,
Harvest Financial Services Limited.

What did you want to do when you left school?
I wanted to be a priest, so I went into the seminary in Maynooth.

How did you enter into the world of compliance?
I was working in the legal department of a global consulting firm and I thought that completing the Professional Diploma in Compliance would be worthwhile. I subsequently ended up working in the legal and compliance department of an international life office and I have been working in compliance departments since and really enjoy the challenges.

What do you consider are the challenges ahead for your industry?
I consider the challenges for the financial services industry is the volume of new regulations which can be open to interpretation, some of which are incorrect when being transposed into Irish law. This is putting pressure on compliance professionals to advise the business in a timely manner on what exactly the new requirements entail.

How would you describe your management style?
I am a bit of a control freak, which can be seen as a benefit for a compliance officer, however, I am learning to delegate to my team. I am always ready to receive feedback and give my colleagues the opportunity to suggest alternative solutions, etc.

What's the most valuable advice that you have been given?
"We make a living with what we get, we make a life with what we give" - it reminds me to have the right work / life balance and to give to those who are less fortunate.

An accomplishment you are most proud of?
Professionally, my academic qualifications. I have 20 certificates and diplomas and hope to finish the Masters in Compliance in the next few years. Personally, my sporting achievements. I have a number from years ago and I continue to win trophies with my team.

> *"'We make a living with what we get, we make a life with what we give.' It reminds me to have the right work / life balance and to give to those who are less fortunate."*

What are you currently watching and listening too?
I am currently watching the Blacklist box set. A few years ago I managed to watch the 24 box set, which took some time and dedication as there are eight series. I am currently listening to soundtracks, such as The Grey, Oblivion, Inception and Solaris.

What's your favourite book of all time and what book changed your life?
I don't have a favourite book. I enjoyed reading the Odessa File by Frederick Forsyth. From time to time I may read a few poems from the Complete Poems of Emily Dickinson. On my bucket list is to read poetry by Jim Morrison.

How do you relax & unwind?
I play tag rugby and walk, usually along Sandymount strand, to relax. I unwind by spending time with family and close friends.

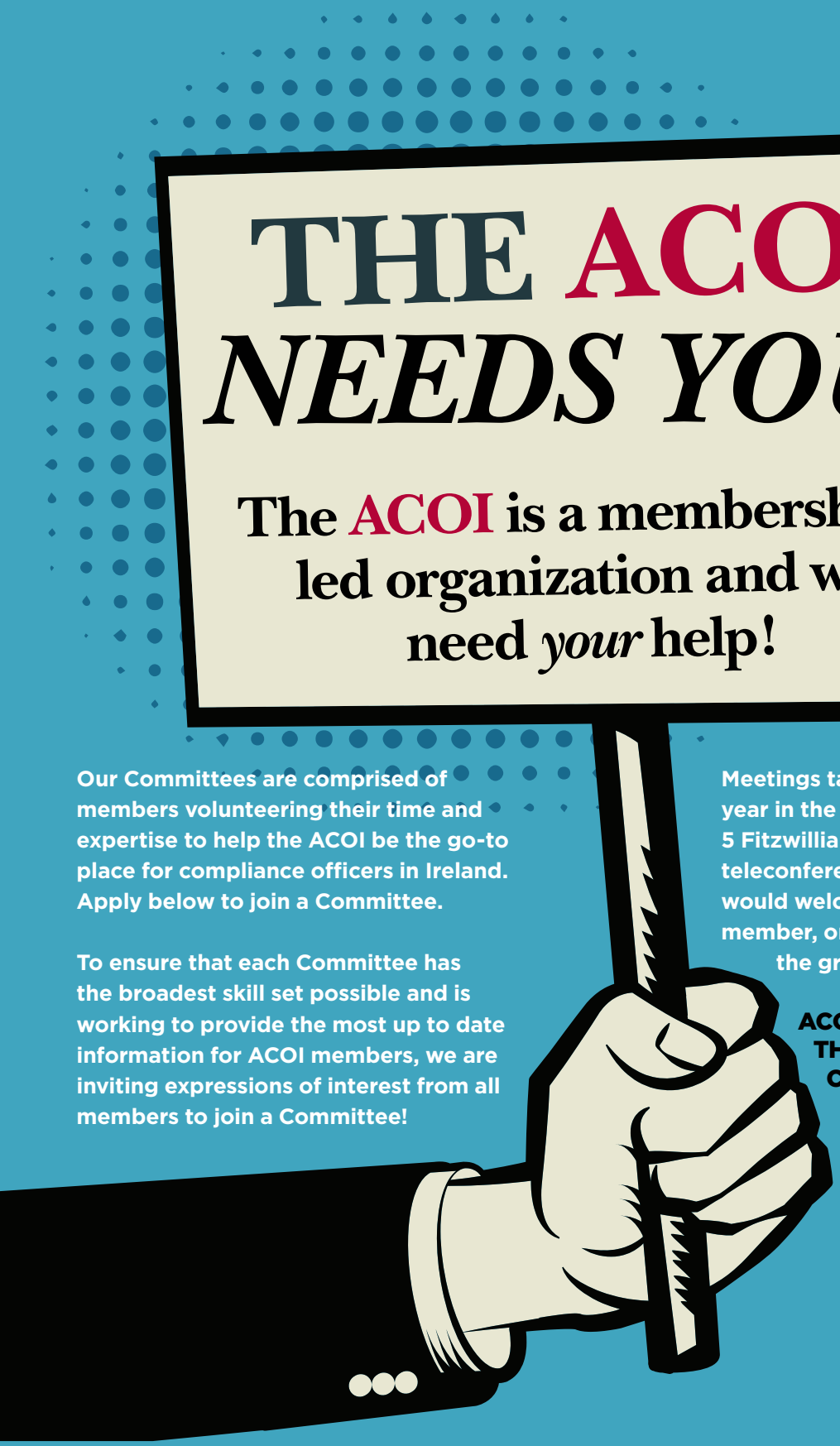
What's your favourite restaurant?
My favourite restaurant is the Avenue Cafe in Maynooth.

Where is your favourite place in Ireland? Leitrim, my home county.

An interesting fact about you?
I can dance, but you can be the judge when you see me in House. ICQ

THE ACOI *NEEDS YOU!*

The ACOI is a membership-led organization and we need *your* help!



Our Committees are comprised of members volunteering their time and expertise to help the ACOI be the go-to place for compliance officers in Ireland. Apply below to join a Committee.

To ensure that each Committee has the broadest skill set possible and is working to provide the most up to date information for ACOI members, we are inviting expressions of interest from all members to join a Committee!

Meetings take place 6 times a year in the Association's offices in 5 Fitzwilliam Square in Dublin 2, teleconferencing is available and we would welcome participation from a member, or members, based outside the greater Dublin area.

ACOI CURRENTLY HOST THE FOLLOWING COMMITTEES:

- Membership Committee
- Ethics Committee
- EPDS - Education & Professional Development Services Committee
- FRAC - Finance, Risk & Administration Committee
- Audit Committee

Any ACOI member who wishes to express an interest in joining one of our Committees can do so by *clicking* the link below.

https://www.acoi.ie/committee/

ACOI
The Association of Compliance Officers in Ireland

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 0200
Email: education@acoi.ie

www.acoi.ie