

# **Ten Key Trends to Watch in Ireland's Regulatory Outlook for 2022**

# **Ireland's regulatory authorities brought 2021 to an end with two statements of intent: a major fine levied on the Bank of Ireland and a “Dear CEO” letter requiring rapid action from Payment and E-Money institutions. Should financial services companies expect more change in the regulatory outlook for 2022?**

In a recent webinar, five experts sought to identify the main trends and developments firms should prepare for in the coming year and beyond. The speakers were:

- Jamie Cooke, Managing Director of fscom and Head of Investments.
- Alison Donnelly, Director and Head of Payments.
- Phil Creed, Director and Head of Financial Crime.
- Nick Gumbley, Associate Director and Head of Cyber Security.
- Russell Burke, Independent Senior Consultant and former employee of the Central Bank of Ireland.

They brought their knowledge and experience from across the financial services sector to identify the implications of upcoming regulatory activity for payment and e-money firms, cyber security, financial crime, innovative payment services, investments and more. This report dives deeper into each of these areas.

The takeaway for companies is that the Central Bank of Ireland (CBI) is likely to be more interventionist in 2022 in its aim to protect consumers and market confidence in the aftermath of the pandemic. The impact is that companies will need to ensure they can demonstrate compliance with the applicable regulations, and this report offers guidance on where to focus those efforts.

# Contents

1. Greater expectations around climate change and ESG	<b>Page 3</b>
2. Creeping regulation of crypto, BNPL and other innovative products	<b>Page 3</b>
3. Heightened scrutiny of operational resilience	<b>Page 4</b>
4. No excuses for lack of consumer protection after COVID-19	<b>Page 7</b>
5. Dear CEO letter sends a wake-up call to Payment and E-Money firms	<b>Page 7</b>
6. Financial crime risks should be mitigated with a business-wide risk assessment	<b>Page 8</b>
7. Recruitment challenges ahead for financial crime compliance	<b>Page 8</b>
8. Regulatory focus on cyber security requires integration with operational resilience	<b>Page 9</b>
9. New tests for investment firms' financial resilience and executive responsibilities	<b>Page 9</b>
10. 2022: the year of regulatory divergence for the EU and UK	<b>Page 10</b>



## 1. Greater expectations around climate change and ESG

Climate change and Environmental, Social and Governance (ESG) factors will be a major focus this year across the financial sector, following governmental commitments at the UN's COP26 summit at the end of last year. The CBI have said that they want to see firms – and their Boards in particular – take more action around climate risks. They should:



Understand and mitigate climate risks.



Carry out scenario analysis to understand impacts on clients and on capital adequacy.



Analyse their business model and understand how it impacts the climate.



Make transparency disclosures to consumers.

There are outsized implications for investment firms here, and asset managers are advised to review their product range to ensure that their products genuinely are green and sustainable. Regulators, investors and consumers are good at spotting 'greenwashing'!

## 2. Creeping regulation of crypto, BNPL and other innovative products

The crypto asset market continues to expand and regulators are trying to keep up by looking more at areas that can be practically regulated and seeking to further develop regulation. They are also likely to stretch existing regulations to address risks from crypto activities – for example, Virtual Asset Service Providers (VASPs) are now covered by Ireland's Anti-Money Laundering (AML) and Countering Terrorist Financing (CTF) framework, which requires these providers to register with the CBI. Likewise, the nascent Buy Now Pay Later (BNPL) sector is coming under greater regulatory attention and regulatory reform is expected to cover this area by the end of 2022.

The sector shouldn't fear regulation or treat it as a bad thing. The CBI's intention is to increase consumer confidence in innovative payment services, and we envisage the sector increasing rapidly over the next three to five years.

### 3. Heightened scrutiny of operational resilience

Operational resilience is a core area of focus for the Central Bank and companies can expect greater scrutiny from the regulator in 2022. Evidence of this came in December 2021 when the Bank of Ireland was fined a record 24.5 million and reprimanded for poor operational resilience and IT failures. This has made Boards sit up and take more notice of this area of their businesses.

The CBI's three pillars of operational resilience are clearly defined, and businesses should be working through each of these. We have found when working with clients that although a lot of expertise exists from an operational point of view, it hasn't necessarily been brought together explicitly under the lens of operational resilience.

Firms recognise the need to focus more resources and attention towards their operational resilience – more than a third of participants in our webinar identified it as their key area of compliance which needs improvement in 2022. But the good news is that they likely already have a wealth of information that supports operational resilience, such as:



Business Continuity Planning documentation.



Documented data flows and processes that govern the security of personal information under the EU's General Data Protection Regulations (GDPR).



Incident Response Planning documentation and playbooks for how to respond to a threat to operations such as a ransomware attack.

All this information can and should be used for operational resilience compliance. Bringing that material together will also lead you to the stakeholders and experts within the company that can help you to understand the supporting processes and give you the foundation for your compliance. In the rush to satisfy regulatory expectations, don't ignore what has already done within your company!

Learn more about operational resilience planning [here](#).



## 4. No excuses for lack of consumer protection after Covid-19

The CBI set out its stall on consumer protection last year when its Director of Consumer Protection said: “Protecting consumers is core to what we do and who we are.” The impact of the pandemic and its risk to consumers’ funds has only raised it up the regulatory agenda. We expect to see more intrusive risk-based regulatory intervention in 2022 when firms are not adhering to their compliance requirements and, as a result, damaging consumer outcomes.

The CBI will want to see evidence that:



Firms have consumer focus at the centre of their culture.



They are identifying and protecting vulnerable customers.



Companies are making effective, transparent disclosures.



They are mitigating risks related to technology and mis-selling.

## 5. Dear CEO letter sends a wake-up call to Payment and E-Money firms

It is clear that Payment and E-Money institutions will feel the weight of a growing regulatory burden this year. The CBI gave notice of its intentions by sending a “Dear CEO” letter to Payment and E-Money firms just before Christmas. Firms’ top priority for 2022 should be dealing with the letter’s requirements by the 31 March deadline.

This means:



Completing an assessment of their compliance with safeguarding obligations and putting in place safeguarding risk frameworks which identify, segregate, manage and protect clients’ funds.



Providing the CBI with a statement confirming this has been completed, with the Board’s approval.



Demonstrating “viable and sustainable” business models.

The priorities in the letter will largely be familiar to firms, although a newer area is the need to embed a wind-up plan within their business model and operational strategy. While there was previously no regulatory requirement or formal guidance on this, firms that are regulated or seeking authorisation are now required to submit these plans. This follows the move of authorisation and supervision responsibility to the Credit Institutions Supervision Directorate last year.

These developments have been met by a wariness across the sector as to where the CBI will go next with its safeguarding provisions. Some have pointed out that the new focus on wind-down planning is confusing, given safeguarding is supposed to protect customers' funds anyway. As a result, some firms are bringing in an external independent consultant to come in and review their compliance. This is a useful exercise which may identify areas that have not previously been considered.

Read more about the Dear CEO letter's requirements [here](#).

Read more about safeguarding [here](#).

## 6. Financial crime risks should be mitigated with a business-wide risk assessment

The 'Dear CEO' letter also targeted financial crime by requiring firms to undertake a business-wide risk assessment. This is fast becoming a cornerstone of good financial crime management. But many firms do not have the risk assessment collateral and deep expertise to develop a comprehensive assessment. If that applies to you, this should be the first area to focus on this year. We know AML and CTF compliance is a top priority for companies – in fact, 42% of participants in our webinar singled this out as the area most in need of improvement for the year ahead. We still see varying levels of quality in business-wide risk assessments, yet it is the foundation from which everything else in your anti-financial crime regime can be built out.

## 7. Recruitment challenges ahead for financial crime compliance

Recruitment and retention of senior personnel in financial crime compliance will be a growing challenge this year, after the CBI split the Pre-Approved Control Function (PCF) 39 function into six new PCF roles related to different areas of compliance. The CBI is removing PCF-15 (Head of Compliance with responsibility for AML and CTF) and redistributing its responsibilities to PCF-12 (Head of Compliance) and the new PCF-52 (Head of AML and CTF). What this shows is that the CBI wants to put more focus on AML and regulatory compliance, with distinct roles for a Head of Compliance and Money Laundering Reporting Officer (MLRO).

The challenge for firms will be finding people of sufficient expertise and seniority. One person can still undertake both roles, but they will need to demonstrate they are suitably qualified and have sufficient capacity – especially with the regulator showing more appetite for carrying out interviews. Firms should invest in identifying, training and retaining the next generation of people to fill these roles.

The CBI will expect to see a candidate's experience and qualifications match the requirements of the role, as well as honesty, integrity, competency and an understanding of the sector.



An MLRO should usually have progressed through the more junior roles and Deputy MLRO while gaining appropriate professional qualifications along the way. They should be able to demonstrate at interview that they understand the products their business offers and how they relate to financial crime risk.

## 8. Regulatory focus on cyber security requires integration with operational resilience

The CBI has focused on cyber resilience for the last couple of years and that will continue in 2022. Its aim regarding IT and cyber security is to increase the “cyber maturity” of financial services institutions by improving the controls and internal systems that enable a more secure operating environment.

Our advice is not to treat cyber security as a standalone issue, but to approach it in lockstep with your operational resilience planning. Too often, we see business functions squirreled away in silos. But if they work together, it leads to better regulatory compliance and supports better delivery of services to customers. The CBI recognises this by making cyber resilience a key component of its “three pillars” model of an organisation’s operational resilience.

The best way to improve your firm’s cyber security is to carry out a baseline of your security by assessing your implemented controls against a recognised framework. Crucially, this should cover your third parties and the way data is shared with them across your business. That will highlight where new controls and improvements are required to improve both your cyber resilience and operational resilience.

## 9. New tests for investment firms’ financial resilience and executive

COVID-19’s effects have increased the risk of impairments caused by customers’ failure to pay, which will impact companies’ capital and liquidity bases. These risks will rise as COVID-related government loans come to an end. The new Investment Firm Regulations require firms to undertake an ICARA process which means they should be undertaking capital modelling and stress testing.

In fact, investment firms face growing regulatory intervention across the board. The Senior Executive Accountability Regime (SEAR) legislation is likely to come into force towards the end of this year. We can learn a lot about SEAR from the implementation of the Senior Managers and Certification Regime in the UK because they are close in design. The key lessons we can take from SMCR is that firms will need to do a significant amount of preparatory work to be ready ahead of SEAR, including:



Mapping out responsibilities across the firm.



Drafting statements of responsibilities for senior management functions.



Identifying those cohort of persons who would need certification.



Identifying the necessary amendments to employees' contracts to be clear about their responsibilities.



Ensure skills gap analysis and training plans are in place.



Carrying out training to ensure that staff are aware of the heightened conduct requirements in SEAR.

This is not all. The Investment Firms Directive (IFD) and Investment Firms Regulation (IFR) came into force last year and we know many firms are still getting to grips with their provisions, especially the changes to the capital reporting.

A key focus for investment firms is the change in the Client Asset Regulations and their extension outside of MiFID firms into credit institutions. The regulator's aim in this regard is to provide more protection for consumers by properly safeguarding their assets.

Firms are also adjusting to the Remuneration Rules and the Internal Capital Adequacy and Risk Assessment (ICARA) requirements of IFR. ICARA takes the requirements for firms to develop a wind-down plan a step further than the ICAAP previously did. Our advice for firms is that developing and maintaining this plan should be treated as an ongoing process, not as a document that you produce once.

## 10. 2022: the year of regulatory divergence for the EU and UK

2022 will almost certainly be characterised by divergence in the EU and UK's regulatory framework. We are already starting to see this in the ongoing Markets in Financial Instruments Directive (MiFID) and Regulation (MiFIR) reviews in both jurisdictions, which are looking at similar areas but will probably arrive at quite different conclusions. Where there is divergence, companies with a presence across Ireland and the UK will have to ensure awareness and compliance with both sets of requirements.

More hints of divergence come with the recent establishment of a Brexit Opportunities Minister in the UK. The Minister, Jacob Rees-Mogg, has identified deregulation as a principal opportunity emerging from the UK's withdrawal. Meanwhile, the EU has made its own moves to give EU banks a competitive advantage by breaking with aspects of the Basel III reforms to allow them to lend to unrated corporates at lower capital levels than UK banks can offer.

Firms seeking authorisation in both Ireland and the UK can expect backlogs to continue this year. But this should not be cause for complacency: firms in the Temporary Permissions Regime (TPR) have been exited from the process because they missed their landing slots or the UK regulator suspected that they didn't really want to be authorised. Applications to be authorised as a regulated entity should be taken extremely seriously in 2022 and beyond.

## In a nutshell: fscom experts' top advice for regulatory compliance in 2022

This report has covered a wide range of regulations and trends across the sector, and companies may be feeling overwhelmed by their compliance to-do lists. So to help focus your efforts, we asked our webinar speakers for their one key piece of advice for the year ahead:



Ireland is a great place for regulated payment providers, however you need to ensure you have a robust strong application to submit to the Central Bank because it expects high standards” – **Russell Burke.**



Update your enterprise risk assessment with particular focus on conduct and culture – preparing for SEAR will take a lot of work and you can't start it too early” – **Jamie Cooke.**



Prepare your wind-up strategy: from our experience of helping firms in the UK with 'wind-down' plans, it takes longer than you'd think” – **Alison Donnelly.**



Forward plan your resource requirements – in the future you will need a Head of Compliance and a MLRO, which are two separate PCF roles” – **Phil Creed.**



Understand and document how your data is shared with third parties and how they meet your security requirements – this again links Operational Resilience to Cyber Resilience” – **Nick Gumbley.**

For advice on any of the topics covered in this report, contact fscom for a free consultation.

## Expertise that adds value

If you would like to find out more about any of the regulatory matters in this report, contact the relevant expert today.



**Jamie Cooke**

Managing Director  
Investments

[jamie.cooke@fscom.co](mailto:jamie.cooke@fscom.co)



**Alison Donnelly**

Director  
Payments

[alison.donnelly@fscom.co](mailto:alison.donnelly@fscom.co)



**Philip Creed**

Director  
Financial Crime

[philip.creed@fscom.co](mailto:philip.creed@fscom.co)



**Nick Gumbley**

Associate Director  
Cyber Security

[nick.gumbley@fscom.co](mailto:nick.gumbley@fscom.co)



**Russell Burke**


Independent Senior  
Consultant

[russell.burke@fscom.co](mailto:russell.burke@fscom.co)



**Let's start a  
conversation.**

Have a compliance question?

 +353 (1) 640 1986

 @fscom1

 @fscom-limited