BDO

IDEAS | PEOPLE | TRUST

Regulatory Update

Payment Services & E-Money Firms

Q2 2024

BDO FS ADVISORY CONTACT POINTS

BDO's Payments and E-money regulatory update summarises the key regulatory developments and emerging business risks relevant for all Payment Institutions and E-money Institutions.

We are working with a multitude of Payments and E-money firms as internal auditors and advisors, giving us a broad perspective on the issues facing the sector. We have insights from our inhouse research team, the Regulators and professional bodies, including the Chartered Institute of Internal Auditors (CIIA), to support your regulatory considerations and activities.

There are a lot of moving parts within the Payments and E-Money sector from ongoing focus on Internal Control Frameworks, Fraud and AML, Digital implementation programs and impending Consumer Duty deadline. Firms need to continue to evolve and meet the ever-increasing regulatory expectations.

Within this publication we have provided a selection of the key themes and areas that we hope will be of value to you and your colleagues. This is not an exhaustive list we will continue to engage in the market and with our clients, to update and inform you of these other areas outside of this publication throughout the year.

Please do share with us any feedback you may have for our future editions and would be happy to discuss any points of interest that may impact your firm or the wider UK and International market.

LUKE PATTERSON

Partner, Internal Audit & Advisory

LEIGH TREACY
Partner, Head of Financial Services Advisory

+44 (0)7890 562 098
leigh.treacy@bdo.co.uk

LUKE PATTERSON
Partner, Internal Audit & Advisory (PSR, EMI & Safeguarding specialist)

+44 (0)7929 058 083
luke.patterson@bdo.co.uk

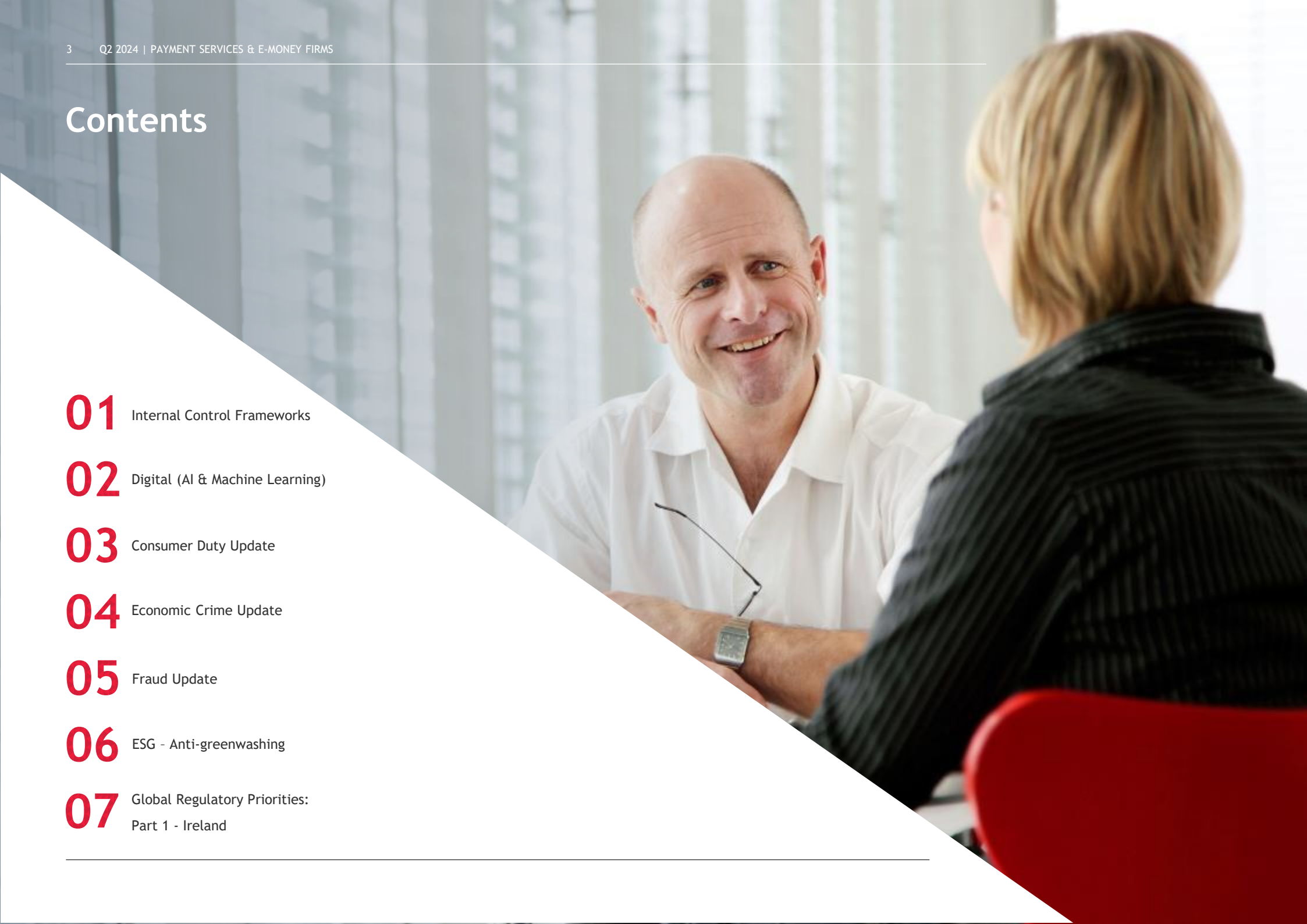
RICHARD BARNWELL
Partner, Regulatory & Advisory

+44 (0)7966 626 128
richard.barnewell@bdo.co.uk

FIONA RAISTRICK
Partner, Economic Crime

+44 (0)7929 057 616
fiona.raistrick@bdo.co.uk

Contents



01

Internal Control Frameworks

Michael Haddon
Principal

michael.haddon@bdo.co.uk

Is your firm's internal control framework really fit for purpose?

A simple question but how confident would you be in your answer? Would it be 'yes, 'sort of' or 'probably not', and what have you based this assessment on?

Our advisory experience, over recent years, has shown us that the internal control frameworks in some small and medium-sized firms tend to be somewhat fragmented, and, where this is the case, are generally not delivering a consistent level of internal control practices across the firm. As a consequence, it is not always clear how internal audit can provide an appropriate level of assurance to Boards to enable them to make comments or disclosures on the effectiveness of the firm's risk management and internal control activities.

Updated Codes - what's new?

Earlier this year, the Financial Reporting Council introduced significant changes to the UK Corporate Governance Code, particularly around internal controls and risk management. The updated Code requires increased director responsibility and accountability for internal controls and transparent reporting. Under the new Provision 29, Boards should monitor their firm's risk management and internal control framework and, at least annually, carry out a review of its effectiveness. The monitoring and review should cover all material controls, including financial, operational, reporting and compliance controls. The Board should provide in the annual report:

- A description of how the Board has monitored and reviewed the effectiveness of the framework;
- A declaration of effectiveness of the material controls as at the balance sheet date; and
- A description of any material controls which have not operated effectively as at the balance sheet date, the action taken, or proposed, to improve them and any action taken to address previously reported issues.

In addition, the CIIA recently issued its consultation paper on its proposed updates to the Internal Audit Code of Practice. Under Principle 11, the paper notes that the provision of an overall opinion from internal audit on the effectiveness of the governance, and risk and control framework (which will support a Board's internal control declaration in line with the updated Corporate Governance Code, noted above).

What does all this mean for Heads of Internal Audit?

HoIAs will soon need to move from providing an overall assessment to an overall opinion. This has shifted the dial considerably on the breadth and depth of the assurance work to be gathered for an opinion to be provided, how much of the Board's public disclosures can be based on the opinion and how matters excluded from the opinion are managed by the HoIA and Audit Committee.

Direction of travel

While the updated Corporate Governance Code only applies to listed companies (or those that adopt it voluntarily), in our view, the key principles and related expectations presents all firms with an opportunity to revisit the strength of their governance arrangements and to assess whether the internal control framework (in its current form) would meet the expectations under Provision 29 as these will very likely be viewed as evolving good practice.

Our experience

From our experience, firms are not always establishing an overarching framework to ensure all internal control related activities are aligned and appropriate integrated. While we usually see well established Risk Management Frameworks and Policies in place, it's unusual to see a comparable and separate (or sufficiently integrated) framework covering internal controls. More specifically, our experience notes the following areas where improvements can be made:

- Fragmented or patchy internal control frameworks
- Inconsistent levels of control discipline and effectiveness
- Less than effective Risk and Control Self-Assessment programmes
- Limited first and second line control effectiveness testing
- Little or no meaningful combined assurance activity.

Is your firm's internal control framework really fit for purpose?

Establishing a baseline

In strengthening an internal control framework, management should use a good practice standard as baseline for designing its target operating model for internal controls. For example, the five key elements under the COSO Internal Control – Integrated Framework: Control Environment/Risk Assessment/Control Activities/Information and Communication/Monitoring Activities).

It should also leverage existing good practices and initiatives, and then cut-back on any elements which are not viewed as proportionate/adding value (and explain why). This should result in a fit for purpose model, supported by a sensible/minimum required level of documentation and evidence of control operating effectiveness.

The overarching framework and related documentation should also cover content such as:

- Scope and Purpose
- Definitions, Standards, Components and Principles
- Roles and Responsibilities
- Governance and Reporting
- Control Assessment/Effectiveness Testing
- Management and Board Certification/Attestation
- Controls Library.

Without a framework, it is more difficult for management and Boards, if required, to attest to the effectiveness of internal controls based on the arrangements in place. In addition, risk and control activities tend to be less mature with relatively low levels of control effectiveness testing other than that carried out by the third line.

Further, as noted, combined assurance activities are rarely developed and built out in a meaningful way. As such, Boards may not be getting sufficient controls assurance from the first and second line.

What should Payment Services and E-Money Firms think about?

Top of the list of priorities under the updated Corporate Governance Code are risk and internal control, and this must also resonate with firms outside of the listing rules.

While some of the updated Principles and Provisions may be quick to implement, effective risk management and internal control is likely to require more time and action (hence the longer implementation date).

A robust risk and internal control framework takes time to be fully embedded and requires input and understanding from across a firm to ensure sufficient maturity of the arrangements. In some cases, a significant shift in culture and behaviours may also be required to deliver on stakeholder needs.

02

Digital Update

SANDI DOSANJH
Partner

sandi.dosanjh@bdo.co.uk

STEVE DELLOW
Director

steve.dellow@bdo.co.uk

Artificial Intelligence and Machine Learning

What is Artificial Intelligence and Machine Learning and what are the associated risks the regulators are focussing on?

Artificial Intelligence ('AI') is the simulation of human intelligence processes by machines, particularly computer systems. It encompasses the ability of a machine to mimic human behaviours such as learning, reasoning, and self-correction. Machine Learning ('ML'), a subset of AI, involves algorithms that learn from data to make predictions or decisions.

AI poses significant risks, including the potential for inherited biases in AI models that can lead to unfair consumer outcomes. Additionally, the lack of explainability in some AI models presents challenges for organisations, necessitating greater transparency and interpretability. The growing dependence on third-party models and data, underscore the need for clear regulatory guidance. Governance risks are also of concern, with a pressing need for regulation and supervision that prioritise consumer outcomes and address ethical considerations.

What should Payment Services and E-Money Firms think about?

Control functions should consider the implications of AI/ML on their firm's operational efficiency, fraud detection, and data analytics capabilities. They should ensure that the firm's use of AI/ML aligns with the regulatory expectations for safety, robustness, transparency, fairness, accountability, and governance.

Furthermore, Internal Audit should keep track of the Regulator's ongoing initiatives, including any guidance or policy instruments that address the unique risks associated with AI/ML. This is critical to anticipate and prepare for any potential effects on financial stability and to ensure that risk management practices are robust and effective.

Additionally, they should assess how AI models are documented, monitored, and reported, ensuring that policies for model development are in place. It's crucial to evaluate the testing and validation of AI outputs, checking for bias and fairness, and understanding the model's relevance and feature engineering.

By taking a proactive and informed stance, Internal Audit Teams can significantly contribute to the responsible and effective integration of AI solutions within their organisations, ensuring that these technologies serve to enhance performance and compliance in equal measure.

Internal audit teams should also consider co-source partners to provide support on activities such as:

- Policy and Governance frameworks to support risk evaluation and oversight of AI and Machine Learning deployment.
- Review of the AI/ML strategy to ensure that it encompasses business intelligence, data strategy, and intelligent automation, and is aligned with the firm's objectives and regulatory expectations.
- Reviewing the architecture and infrastructure on platforms such as Microsoft Azure, to enable the deployment of advanced AI/ML capabilities.
- Delivering tailored AI/ML solutions, from transforming data to enhance usability to developing sophisticated analytics and machine learning models. This includes fraud detection systems and regulatory reporting, ensuring specific business outcomes or regulatory requirements are met.
- Reviews of AI/ML models, assessing governance, documentation, monitoring, and reporting. This includes evaluating models for bias and fairness, ensuring relevance, and training primary users, ultimately safeguarding the impact on clients and aligning with regulatory standards.

If you have any queries regarding the role of Internal Audit in providing assurance over AI and/or machine learning or would like to discuss BDO's experience in supporting IA teams on this topic, please contact Sandi Dosanjh, Steve Dellow or Gopal Tarakad.

03

Consumer Duty Update

ALISON BARKER
Special Adviser

alison.barker@bdo.co.uk

Preparing for the Board's first annual review of Consumer Duty

As firms start to prepare for their annual Board review, we look at some of the key points to consider and think about practical considerations as well as how smaller firms may want to approach their annual review.

How should Payment Services and E-Money Firms prepare the Board to review consumer outcomes?

The FCA's Final Guidance states that "A firm's governing body should review and approve the firm's assessment of whether it is delivering good outcomes for its customers which are consistent with the Duty and agree any action required, at least annually".

The FCA expects the annual review to focus on:

- the results of the monitoring that the firm has undertaken to assess whether products and services are delivering expected outcomes in line with the Duty,
- any evidence of poor outcomes, including whether any group of customers is receiving worse outcomes compared to another group, and an evaluation of the impact and the root cause
- an overview of the actions taken to address any risks or issues
- how the firm's future business strategy is consistent with acting to deliver good outcomes under The Duty

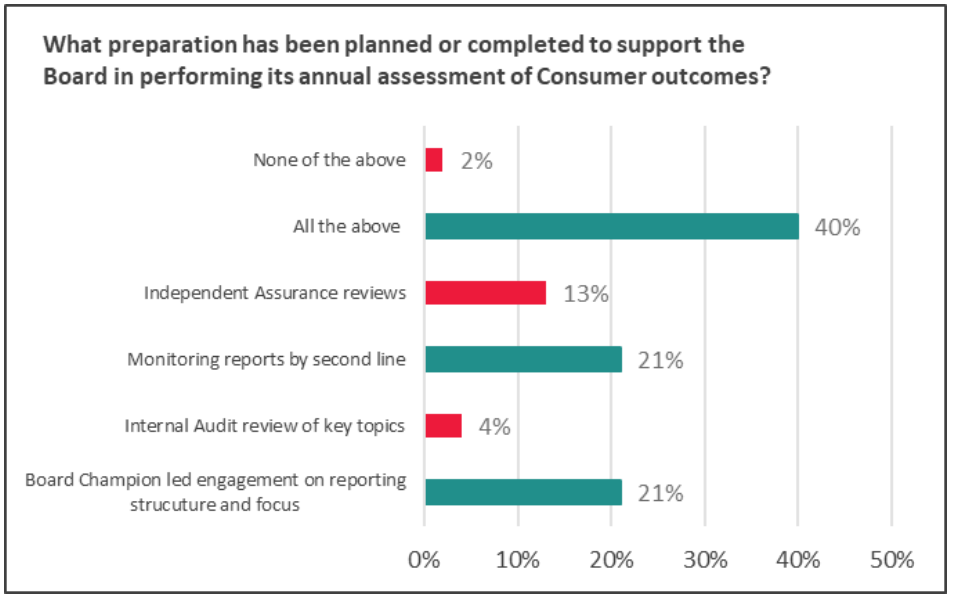
The purpose of the Board Report is to ensure banks and building societies are using meaningful MI to identify gaps and progress actions on a regular basis. The Board report enables the Board to challenge the executive on progress in delivering agreed consumer outcomes, and that organisation shifts to outcomes-based approaches. The annual review provides the Board with an opportunity to decide what to do with the data and what decisions to make. From our work, we see stronger Board reporting also looking at future strategy and direction as well as an assessment of current consumer outcomes.

Each Board is different, therefore thought should be given on how best to engage. This includes the right timing in the board cycle, the right reporting format, and an optimal level of detail. Ultimately the report should enable the Board to assess the judgements made about the quality of outcomes and understand actions taken or due. Where appropriate, that should include preparedness for implementation of the Consumer Duty for closed books.

Firms will have had different approaches to Board reporting over the last year. Some may have engaged sub committees to scrutinise risks and actions related to consumer outcomes. Some may have had regular reporting, some smaller firms may have had less frequent reporting. Consolidating reporting with a final assessment may be a sensible approach.

The Board Champion role is key in the drive towards outcomes-based approaches, utilising data, the continual focus on customers and cultural change. The Board Champion should be engaged early to help shape and challenge the report, although remembering this is an executive report to the Board.

At our Consumer Duty Champions event in January, we polled the audience about the preparation for the Board reports.



While 40% of respondents confirmed that all of the above measures, including IA's review of key Consumer Duty topics, were in place; that would suggest that only 4% of the remaining respondents have had review from the Third Line on this critical area. That is a concerning picture. Internal Audit teams need to factor in an appropriate level of review over the annual assessment of consumer outcomes if not already in place. The Regulator has repeatedly emphasised the importance of this Duty.

The FCA helpfully published ten questions Boards should consider asking to help focus the Annual review conversation. These questions consider purpose, culture, and governance as well as delivery of outcomes and actions taken.

The structure of a report to the Board could reflect these questions and enable a structured discussion and this is an approach smaller firms might find helpful in preparing their Board report.

Preparing for the Board's first annual review of Consumer Duty

1. Are you satisfied your products and services are well designed to meet the needs of consumers in the target market, and perform as expected? What testing has been conducted?
2. Do your products or services have features that could risk harm for groups of customers with characteristics of vulnerability? If so, what changes to the design of your products and services are you making?
3. What action have you taken as a result of your fair value assessments, and how are you ensuring this action is effective in improving consumer outcomes?
4. What data, MI and other intelligence are you using to monitor the fair value of your products and services on an ongoing basis?
5. How are you testing the effectiveness of your communications? How are you acting on these results?
6. How do you adapt your communications to meet the needs of customers with characteristics of vulnerability, and how do you know these adaptions are effective?
7. What assessment have you made about whether your customer support is meeting the needs of customers with characteristics of vulnerability? What data, MI and customer feedback is being used to support this assessment?
8. How have you satisfied yourself that the quality and availability of any post-sale support you have is as good as your pre-sale support?
9. Do individuals throughout your firm – including those in control and support functions – understand their role and responsibility in delivering the Duty?
10. Have you identified the key risks to your ability to deliver good outcomes to customers and put appropriate mitigants in place?

What should Payment Services and E-Money Firms think about?

Control functions should scrutinise reporting, the quality of metrics, judgements made, and actions taken. This should demonstrate that testing is fully operational and effective, and act as a measure of how well consumer duty principles are embedding across the organisation.

Finally, firms should allow enough time. An early 'dry run' might help flush out any unanticipated challenges, and the Board might appreciate a first review with further review once feedback has been addressed.

04

Economic Crime Update

KAREN MONKS
Senior Manager

karen.monks@bdo.co.uk

VLADIMIR IVANOV
Senior Manager

vladimir.ivanov@bdo.co.uk

Wolfsberg Principles for Auditing Financial Crime Risk Management

On 27 March 2024, the Wolfsberg Group ('the Group') published the Principles for Auditing a Financial Crime Risk Management ('FCRM'), which sought to build on the Wolfsberg Factors, which were published in 2019, and are key to what the Group believed should underpin any financial crime programme. The Principles seek to further illustrate the important role that Internal Audit has in assessing the comprehensiveness and effectiveness of the FCRM programme.

Factor 1: Complying with Financial Crime Laws and Regulations

Principle 1: As a baseline, Internal Audit should assess whether the business can demonstrate that its governance documents address the requirements of all relevant local laws, regulations and regulatory requirements and assess whether the business has an effective set of controls to ensure adherence to these requirements.

Expected Measures

- The business can evidence that local financial crime laws and regulations have been addressed in key governance documents.
- The business can evidence that controls mapped to these elements of the governance documents are designed and operating effectively.
- The business can evidence a sufficiently governed process to assess the adequacy of the FCRM programme in addressing regulatory requirements.

Factor 2: : Establishing a reasonable and risk-based set of controls to mitigate the risks of a financial institution being used to facilitate illicit activity.

In order to develop appropriate FCRM systems and controls, the business must understand the inherent financial crime risks in its business strategy and operating model; the expectations of its regulators; and its own risk appetite.

Principle 2: Internal Audit should evaluate whether the business has a well-designed, reasonable and risk-based set of controls, and then assess the effectiveness of the controls.

Expected Measures

- The business can evidence that its set of controls is designed to provide reasonable coverage that is proportionate to the risks identified in its risk assessment documentation.
- The business can evidence that the set of controls is effective.
- The business can evidence a sufficiently governed process for changes to its set of controls and that such governance gives appropriate consideration to financial crime risk.

Factor 3: Providing highly useful information

The final Factor seeks to focus on the effectiveness and quality of the information provided by the business to the regulator, law enforcement and government agencies, in respect of financial crime.

Principle 3: A Firm may choose to establish quantitative and/or qualitative indicators relating to the sharing of highly useful information to relevant government agencies.

Expected Measures

- The business may consider developing a credible and reasonable set of indicators upon which to assess its performance in providing highly useful information to relevant government agencies in defined priority areas.
- The business can evidence that it is collecting the indicators it has set for itself.
- The business can evidence oversight through formal governance of its self-assessment on its provision of highly useful information to relevant government agencies.

What should Payment Services and E-Money Firms think about?

The Principles seeks to illustrate how an effective Internal Audit framework can enhance and assist in ensuring that the business has an appropriate FCRM framework in place to manage and monitor its financial crime risk. The FCA has been clear that combatting financial crime remains a key priority and a key control for this is ensuring that businesses have an appropriate third line of defence.

Firms should ensure that the current framework is aligned to the Wolfsberg Principles. In particular does the current testing plan assess:

- Whether the current FCRM framework aligns to the local laws and regulations and meet the minimum regulatory expectations.
- How has the control framework been mapped to meet local legal and regulatory requirements.
- Where there has been any deviation from Group policy, has this been documented and appropriately monitored.
- Where there have been enhancements or changes to the control framework, has there been appropriate governance over the process and do changes made ensure that the business continues to maintain a reasonable risk-based set of controls.
- How is the data utilised in MI packs and presented to senior management validated to ensure that it is accurate.

05

Fraud Update

SALLY FELTON
Director

sally.felton@bdo.co.uk

Combining fraud risk and anti-money laundering controls – is it time?

In the fast-paced world of financial transactions, payments and e-money firms must be vigilant in safeguarding their operations from both money laundering and fraud. These two areas, whilst distinct in nature, often overlap creating a complex web of risks that can threaten the integrity and stability of financial institutions. The FCA underscores the importance of robust controls in both domains, advocating for a unified approach to detect prevent and manage financial crime.

One example where combining controls could be beneficial in a particular fraud type would be in Authorised Push Payment (APP) scams. The Payment Services Regulator's new rules around APP Fraud aim to provide better protection for customers and make it clearer who is responsible when things go wrong. The rules are all about accountability and customer protection, just like AML controls and are designed to safeguard customers from financial harm.

Why this is important

There are many reasons why integrating these controls are not just beneficial but essential for a payments or e-money firm.

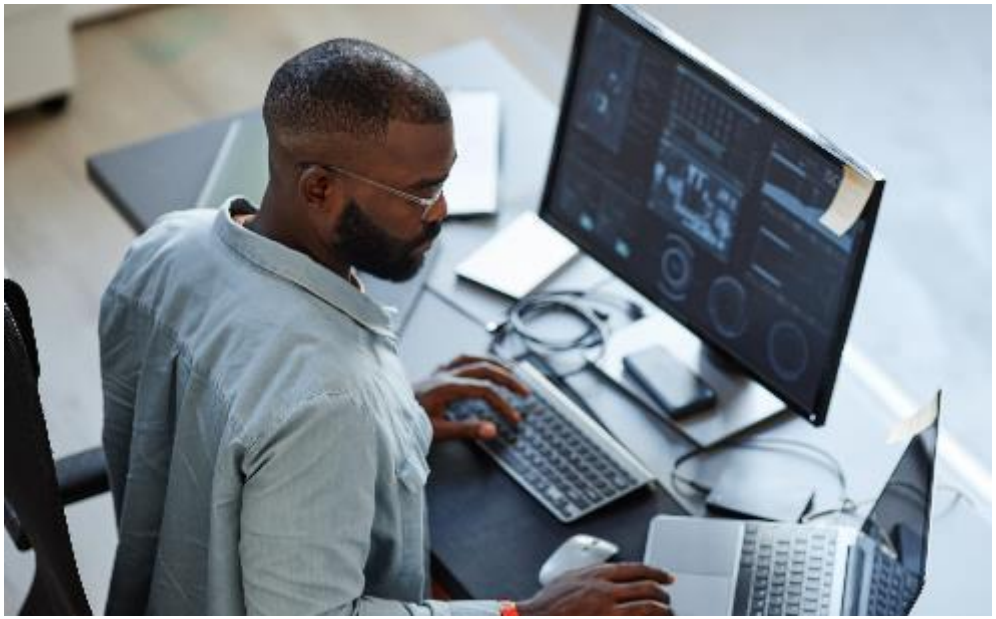
- Combining the two controls can lead to a more streamlined monitoring process which can allow for sharing intelligence and resources which can in turn improve the detection of suspicious activities which may indicate either money laundering or fraud
- Integrated controls ensure holistic view of the risks faced by the firm. This comprehensive perspective is critical for identifying any vulnerabilities which could be exploited for financial crime.
- The FCA encourages firms to adopt a risk-based approach to managing economic crime. An integrated system will align with this guidance, helping to ensure the firm meets its regulatory obligations and avoid potential fines or other penalties.
- Maintaining separate systems for preventing and detecting both money laundering and fraud controls can be costly. Integration can reduce operational costs by eliminating duplicate effort and systems.
- A firm which effectively manages its financial crime risk is more likely to maintain a good reputation with its shareholders, customers, suppliers and the public in general.

The integration of anti-money laundering and fraud controls is not just a strategic move but a necessity in today's regulatory, legislative and operational landscape. It enhances the effectiveness of a firm's risk management approach and positions it to respond swiftly and decisively to potential threats.

What should Payment Services and E-Money Firms think about?

Payments and e-money firms should be considering a thorough review of their controls, consulting with compliance and risk management experts and developing an integrated framework that aligns with the FCA's guidance. My colleagues expand on this issue further, overleaf, with respect to the Wolfsberg Principles for Auditing Financial Crime Risk Management.

By taking these steps firms can ensure they remain on the front foot in the fight against fraud and financial crime rather than reacting to instances when they occur.



06

ESG Update

ADAM SOILLEUX
Director

adam.soilleux@bdo.co.uk

GLORIA PEREZ TORRES
Associate Director

gloria.pereztorres@bdo.co.uk

FCA's Final Guidance on Anti-greenwashing: Are you ready for 31 May?

On 23 April 2024 the FCA published the Final Anti-greenwashing Guidance to help firms understand and comply with its Handbook rule ESG 4.1.1R(1) and ESG 4.3.1R. This follows the publication of the FCA's Sustainability Disclosure Requirements and Labelling Regime ("SDR") published on 28th November 2023 which introduced an Anti-greenwashing Rule (AGR).

The final guidance and accompanying press release by the FCA confirms the 31 May 2024 as the date of entry into force for the rule. By then, authorised financial institutions will need to make sure that they are not in breach by making unfair, unclear, or misleading claims about their products and services.

What this means for the financial services sector?

The FCA has made clear their expectations of firms by publishing the final guidance. Despite the final guidance being published just over a month before the 31 May deadline, given the prior signposting by the FCA of the introduction of this rule, we expect that the FCA will not accept any excuse regarding lack of time and/or clarity on how to comply.

It is now confirmed that from 31 May, the FCA will have powers to challenge and potentially punish firms if it considers that communications to clients or persons in the UK are in breach of the AGR, for example by firms making exaggerated or misleading sustainability-related claims about their products and services.

The final guidance reflects feedback from firms following a consultation adding additional detail around scope, applicability, use of imagens, interrelation between the AGR and the SDR's naming and marketing rules, and the provision of additional examples of good practices which they expect firms to implement.

How should firms interpret the 31 May deadline?

Firms should be compliant as of 1 June 2024. Firms with products and services that promote environmental and social characteristics should already have started preparations to meet the deadline, based on the draft guidance.

Additionally, firms servicing retail customers should already have conducted similar exercises reviewing the clarity, comprehensibility and fairness of its product and service-related communications as part the implementation of the Consumer Duty regime. There is also an argument that similar requirements already exist for all authorised firms in respect of being clear, fair, and not misleading to customers.

What should Payment Services and E-Money Firms think about?

Those firms that have only recently introduced sustainability-related products and services, and who have not had to extensively implement the Consumer Duty or have not made any preparations to date may struggle to assure compliance with the AGR by the 31 May.

Carrying out sufficient depth of analysis to ensure compliance with the AGR properly is not a small task as this lots of aspects of the business and functions across the three lines of defence.

By the end of May, control functions in the firm should have:

- considered the risks for themselves, have them recognised by the Board and Senior Management and ensure that they are being dealt with by the business; and
- actively reconsidered the audit plan for what they should be reviewed in this cycle over AGR compliance.

Where financial institutions regulated by the FCA do not promote any environmental and social characteristics of products and services naturally have less to do but should still ensure that their wider firm-related sustainability claims are accurate and can be substantiated.

The FCA has reminded firms that the CMA and ASA's guidance and FCA Principles 6 and 7 or, as relevant, the Consumer Duty (Principle 12 and the rules in PRIN 2A), already apply to sustainability-related claims that a firm may make about itself as a firm therefore this will require analysing those rules against current practices, which could be a task for the compliance which can then be assured by the internal audit function.

In general, the lead up is not a long period of time, and firms will need to focus on meeting the requirements to avoid regulatory risks.

07

Global Regulatory Priorities Series: Ireland

CIARA HANRAHAN
Director, FS Risk & Advisory

ciara.hanrahan@bdo.ie

Global Regulatory Priorities - Part 1: Ireland

We have introduced a new section within the regulatory priorities, 'BDO Global'. This aims to bring relevant regulatory insights from around the world, as we recognise our clients are not UK only, but a lot of firms are Global and servicing a global client base.

BDO's International presence has a global footprint, reach and international team. BDO International have presence in 167 countries around the world covering over 86% of the world (shown below). Every edition we will be sharing different insights from our international team.

In this edition, BDO Ireland, one of our closest neighbours and whom our UK team works hand in hand with, provide an update on key regulatory issues impacting their territory.

BDO Ireland:

Revenue : €81.97m
Offices: 4 - Cork, Dublin, Limerick (Belfast)
Partner: 39
Staff: 600+

https://www.bdo.ie/en-gb/bdo-ireland

Global Regulatory Priorities - Part 1: Ireland

The Payment and E-Money sector in Ireland has seen significant growth over the last seven years. There are now 51 firms regulated by the Central Bank of Ireland (CBI), with many more applications in the pipeline. As of December 2023, there is approximately €8bn held in safeguarded funds, protecting consumers against the crystallisation of unacceptable risks in the eyes of the CBI. As outlined by Elizabeth McMunn, Director of Banking, Payments, and Credit Union Supervision, in her speech to the industry on 29 February 2024, the stability and reliance of the sector is a key focus of the CBI.

With this growth of the sector also comes the need for an increased supervisory focus from the CBI, with an acknowledgement that the regulator must evolve and adapt its approach to regulating and supervising the sector. Innovative firms can develop new technologies giving substantial advantages to consumers and the broader marketplace. However, these new innovations also bring new risks to consumers and the wider economy as a result. One of the key priorities for the CBI is to create a regulatory environment that is suitable, "remains risk-based," and "is led by judgement and focussed on the outcomes we are seeking to achieve".

In order to achieve this outcome, the CBI mentions the following four principles as key priorities:

- Safeguarding;
- Operational Resilience and Outsourcing;
- Governance, Risk Management, and Anti-Money Laundering and Countering the Financing of Terrorism; and
- Business Model and Financial Resilience.

Safeguarding

The safeguarding of customer funds is a key focus of the CBI, as demonstrated by the "Dear CEO" letter issued in January 2023. The letter was sent with the purpose of reaffirming their supervisory expectations, both firm-specific and sector-wide, and to enhance transparency around the CBI's approach to, and judgements around regulation and supervision. The focus on safeguarding funds is not just a key priority of the CBI. In the UK, the Financial Conduct Authority (FCA) has told payment firms that their "top priority" should be ensuring that their customers' money is safe.

Operational Resilience and Outsourcing

We have seen from other instances across the banking section that when key infrastructure to a firm is impacted it can have detrimental impacts on customers and the sector as a whole. As the industry has a high reliance on technology, the CBI expects that firms have the ability to respond to, adapt to, and be able to recover quickly from disruptions. Operation resilience should be front of mind for a firm's Board and Executive team.

Governance, Risk Management, and Anti-Money Laundering and Countering the Financing of Terrorism

Given the industry's fast-paced growth, the CBI believes that firms with strong governance and risk management foundations are best placed to reap the benefits of growth and innovation in the sector. As the sector expands at a rapid pace, so do the potential risks to customers and the sector. The inherent risks of money laundering (ML) and terrorist financing (TF) associated with the sector are high and the CBI has noted shortcomings in the industry in understanding the risk of ML and TF.

Business Model and Financial Resilience

Change within the Payments & E-Money sector is driven by innovation, evolving regulations, and emerging technologies. Firms and boards are ultimately responsible for managing the risks to which they are exposed. And while the CBI will "serve the public interest by maintaining monetary and financial stability, while ensuring that the financial system operates in the best interests of consumers and the wider economy", the responsibility of staying agile, diverse, and resilient remains with the individual firms.

FOR MORE INFORMATION:

Luke Patterson

+44 (0)7929 058 083
luke.patterson@bdo.co.uk

www.bdo.co.uk

XXXXXXX