IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

January & February 2024

BDO FS INTERNAL AUDIT CONTACT POINTS

BDO's Banking & Building Societies Update summarises the key regulatory developments and emerging business risks relevant for all banks, building societies and, where flagged, for alternative finance providers (i.e., peer-to-peer lenders, card providers, E-money services providers and debt management companies).

Our FS Advisory Services team are working with more than 50 banks and building societies as internal auditors and advisors, giving us a broad perspective on the issues facing the sector. We have aggregated insights from our in-house research, client base, the Regulators and professional bodies, including the Chartered Institute of Internal Auditors (CIIA), to support your audit plans and activities.

In this month's edition, we have also included some broader hot topics that would be of interest to Heads of Internal Audit and for the awareness of their senior management.

We hope this pack provides value to you and your colleagues; please do share with us any feedback you may have for our future editions.

LEIGH TREACY
Partner

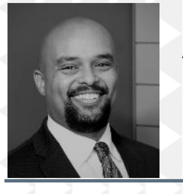
+44 (0)7890 562 098
leigh.treacy@bdo.co.uk

RICHARD WEIGHELL
Partner

+44 (0)7773 392 799
richard.weighell@bdo.co.uk

CHRIS BELLAIRS
Partner

+44 (0)7966 626 128
christian.bellairs@bdo.co.uk



BRUK WOLDEGABREIL
Associate Director

+44 (0)7467 626 468
bruk.woldegabreil@bdo.co.uk

Contents

01

2024 Global Internal Audit Standards

LUKE PATTERSON
Partner

luke.patterson@bdo.co.uk

2024 GLOBAL INTERNAL AUDIT STANDARDS: WHAT SHOULD HEADS OF INTERNAL AUDIT THINK ABOUT?

Implementing the New Global Internal Audit Standards

On the 9 January 2024, the long-awaited [2024 Global Internal Audit Standards] (the "Standards") were published. The incoming Standards will become effective on 9 January 2025 and conformance is required from the effective date.

Firms have a 12-month transition period from the issuance date. Our FS Internal Audit practice has already started to support firms commence their gap analysis between their existing Internal Audit Methodology and the incoming Standards to identify gaps and embed enhanced processes to meet the new requirements, either as part of their EQA or as a standalone exercise to help the IA function's preparations.

The implementation of the incoming Standards affords Internal Audit functions with the opportunity to reassess the function's role, mandate, position in the firm, and enhance the impact, standing and value that the function provides.

The new Standards are organised into 5 Domains and 15 Principles to enable an Internal Audit function to provide and evidence their effectiveness. While most of the incoming Standards overlap with the current (2017) standards, there are new aspects that Heads of Internal Audit should be aware of, such as the more prescriptive requirements highlighted below. The five domains covered under the incoming Standards, with new principles highlighted:

- Domain I: Purpose of Internal Audit
- Domain II: Ethics and Professionalism (New: Principle 5)
- Domain III: Governing the Internal Audit Function (New: Principle 6 and 8)
- Domain IV: Managing the Internal Audit Function
- Domain V: Performing Internal Audit Services (New: Principle 13, 14, and 15)

The Standards use the words "must", "should" and "may" to specify the required, recommended and preferred practices for implementation respectively. For example, the 2017 standards used the term "shall" with respect to the Code of Ethics; the incoming standards use the term "must" emphasising the mandatory element of the requirement to comply with the Code of Ethics.

Where internal auditors may be unable to conform to specific parts of the Standards, they should implement alternative actions to meet the intent of the associated Standards.

New Standards driving positive change

The incoming Standards require firms and Internal Audit functions to think and operate differently in some key areas.

We have pulled out some of the key changes in the Standards from each of the Domains, for you to consider, and we would welcome a discussion to share further thoughts and considerations for your Internal Audit function.

As a non-exhaustive list, changes include:

- More prescriptive requirements for the board to discuss, review and approve the audit mandate at least annually and have an Internal Audit Charter with prescriptive areas detailed within the New Standards. In addition, the board has a responsibility to establish and protect the Internal Audit function's independence.
- Chief Internal Audit executive is responsible for managing the IA function, developing an effective IA strategy, plan and methodologies that supports the achievement of the firm's objectives.
- Exercise Due Professional Care includes the requirement for internal auditors to maintain professional scepticism, demonstrate competency and maintain and continually develop their competencies.
- New requirements to develop an approach to build relationships and communicate with stakeholders via formal and informal channels throughout the audit plan and within each engagement.
- The Head of Internal Audit must establish a methodology for internal quality assessment that includes communication with the board annually about results relating to planning, track and measuring performance, including compliance with the New Standards.
- The requirement for an external quality assessment may be met periodically though a self-assessment with independence validation. However, an independent validation does not fully replace the requirement for the Internal Audit function to conduct external quality assessments.

There will also be a separate series of "Topical Requirements", i.e., good practice guides, being developed by the IIA to cover specialist areas of auditing (e.g., Cyber, Fraud, ESG etc) as part of the incoming Standards.

IA functions should consider their approach for the incoming Standards and incorporate a gap analysis within the transition period as part of their annual self-assessment or within their External Quality Assessment if taking place this year.

BDO can support your team by sharing insight on good practice happening within the market, undertake a gap analysis against the incoming standards, develop a strategy for embedding the requirements to the standards, including process and control enhancements to evidence the function's conformance by the effective date.

02

2024 Regulatory Priorities

ALISON BARKER
Special Adviser

alison.barker@bdo.co.uk

Hot topics for 2024 - The Regulators' Outbox

Banking & Building Societies

Regulatory Initiatives Grid

The Regulatory Initiatives grid describes the pipeline of initiatives that are in train to enable industry to plan for implementation.

Regulatory Initiatives Grid - November 2023

There are 143 initiatives on the grid. The FCA lead just over 50% and the PRA 16%. The remainder are split between HMT, BOE, TPR, FCR, PSR and ICO.

The political, geopolitical, and economic environment remains unsettled. US presidential elections take place in November. This is also possibly a general election year in the UK, and we could see the regulatory agenda change if there is a change in Government. The bigger change in agenda may, therefore, be in 2025.

What should Internal Audit teams think about?

Some of the significant policy initiatives planned this year that Internal Audit teams should have on their regulatory radar are as follows:

ESG

ESG continues to be a heavy part of the regulatory agenda given its strategic importance to UK financial markets and growth. The FCA published the sustainability disclosure requirements (SDR) at the end of 2023, which includes a universal anti-greenwashing rule for all FCA authorised firms. My colleagues, Adam and Gloria, dive deeper into this topic in part 4 of this update, further below.

Additionally, a new voluntary code on ESG data and ratings was published in December 2023. Further consultation will come from other government departments as well. There is also a range of other enablers such as consultation on climate transition plans; FRC stewardship code; Green taxonomy; and sustainability corporate reporting standards.

There is also an expected consultation covering ESG disclosures and MIFIDPRU clarifications for FCA investment firms. BDO has more detailed information and ESG updates here.

A final Policy Statement on Diversity and Inclusion in the Financial Sector is expected in H1 2024, these proposals will support greater diversity and inclusion across the sector, for example requiring firms to report additional diversity and inclusion related data.

Hot topics for 2024 - The Regulators' Outbox

Banking & Building Societies

Crypto

The evolving crypto market and how to regulate it continues to be a topic regulators are grappling with globally. The UK Government's ambition is for the UK to become a global hub for crypto assets. This is a long haul.

Initial proposals for regulating a broad suite of crypto activities in the UK were published in 2023. Treasury intend to lay secondary legislation in 2024 which will be accompanied by FCA publications.

Stable Coins

The regulators published Discussion Papers and follow on FCA consultation papers (CP) from both the Bank and FCA will be published circa H2 2024.

The timing of the FCA CP is subject to Treasury secondary legislation being laid.

Scams - Authorised Push Payment (APP) scam prevention

The PSR is looking at measures to help prevent APP scams and protect victims.

There are several policy statements expected in 2024 to finalise the reimbursement model and we can expect to hear about the implementation date for the new model.

Access to cash and cash savings

The FCA plans using a range of regulatory tools, particularly the Consumer Duty, to help achieve a competitive cash savings market and better outcomes for savers.

A report was published in July 2023 on competition and consumer outcomes in the cash savings market. This includes a 14-point action plan with a range of actions for the FCA and firms, as well as voluntary industry commitments.

A Consultation was published at the end of 2023.

Supervisory work on consumer engagement plans and fair value assessments for some of the lowest paying easy access accounts is underway. During H1 2024, FCA will complete analysis on the contribution of cash savings to profitability.

Hot topics for 2024 - The Regulators' Outbox

Banking & Building Societies

Consumer Duty

As a reminder, the Consumer Duty comes into force for closed products on 31 July 2024. Closed products are products or services no longer on sale for new customers or available for renewal by existing customers.

The supervisory agenda over the last six months has been intense and we can expect to see a continued focus on consumer outcomes and practices the FCA sees as unfair. Firms need to be on top of FCA communications, their own outcomes assessments and reporting to spot issues and act as needed. The Board should review whether the firm is meeting consumer outcomes by the first anniversary of the Consumer Duty implementation date, 31 July 2024.

Prudential framework for non-systemic banks and building societies

The Liquidity and disclosure requirements for the simplified regime for non-systemic banks and building societies is expected in H1 2024.

For firms meeting the scope criteria, this will provide further clarity on the proposals.

Arrangements for this transitional regime will be published along with the Basel 3.1 Near-Final Policy Statements.

Treasury is planning to consult on the necessary revocations in H1 2024.

Buy Now Pay Later (BNPL)

The long-awaited legislation and subsequent regulatory consultations are still on the Grid, however there are no estimated dates given, therefore, timing remains uncertain.

Unregulated BNPL still remains outside the scope of regulation although the FCA has used powers under other consumer legislation to ensure consumer contracts and advertising are fair and clear.

Accessing and using wholesale data

Data is the new gold, and this market study is designed to look at how the market is operating and importantly how participants can access data.

This market study is assessing potential competition issues about benchmarks, credit rating data and market data vendors.

The market study update was published on 31 August 2023 and the market study report should be published on, or before, 1 March 2024 at the latest.

This might be one to watch.

03

Artificial Intelligence in Financial Services

JENNIFER CAFFERKY
Associate Director

jennifer.cafferky@bdo.co.uk

Artificial Intelligence: Opportunity, risk, and regulation in financial services

Intelligent systems such as AI and Machine Learning have become increasingly utilized by firms within the Financial Services sector. The growing significance of AI, highlighted by innovations such as ChatGPT, is evidence of the ongoing digital transformation that the industry is experiencing. In the market, we have observed an increasing number of firms utilising AI in a myriad of ways, including the analysis of Big Data in identifying consumer trends, predicting potential financial downturns, and assessing loan repayment capabilities of borrowers.

In this article, we explore the opportunities and risks associated with the use of AI, the current regulatory landscape, and key considerations for FS firms.

What are the potential Opportunities and Risks associated with AI?

There are undoubtedly significant opportunities as a result of recent AI advances, but there are also a number of risks that firms should be aware of as they look to implement AI-based solutions within their businesses.

Opportunities:

- Enhanced Data Analysis and Insights: AI algorithms can process vast amounts of data at high speeds, allowing firms to generate actionable insights from complex datasets. This can result in better decision-making processes and a deeper understanding of market dynamics and consumer behaviour.
- Automated Customer Service: Chatbots and virtual assistants can now provide 24/7 customer service, improving client interactions, particularly in answering FAQs. This will reduce the need for human intervention, which can help redirect focus for addressing complex queries.
- Improved Risk Management: Predictive algorithms can identify potential financial risks, helping firms in proactively assessing and mitigating their risk exposures.
- Fraud and money laundering Detection and Prevention: AI can be used in real-time to identify and flag irregular patterns or transactions in high volume transaction processing, significantly increasing the likelihood of identifying potential fraud events and money laundering breaches.
- Operational Efficiency: Automating manual, time-consuming and routine tasks can result in higher productivity, efficiency gains, and cost savings.
- Tailored Financial Products: By analysing customer data, firms can offer personalised financial products and services, enhancing the user experience and increasing client retention.

Risks:

- Data Privacy: As AI relies heavily on data, protecting data privacy is of heightened importance, with the potential for misuse of personal information and potential cyber security breaches.
- Over-reliance on Automation: Heavy reliance on AI may lead to missed human insights, resulting in suboptimal decisions or overlooked risks.
- Job Displacement: As AI continues to automate various tasks and processes, there is a heightened risk to job security.
- Underlying Data Risks: AI models are only as good as the underlying data that supports them; incorrect or biased data can lead to inaccurate predictions or suboptimal decisions by AI models.
- Systemic Herd Behaviour: Where many firms adopt similar AI models, there is an increased risk of ‘herd behaviour’ within financial markets, possibly intensifying market volatility and sensitivity to shocks.
- Ethical and Inclusion Concerns: AI-driven decisions, especially without proper oversight, could lead to unfair, biased or discriminatory outcomes. Firms need to consider their reputation, impact on customers, and regulatory compliance, particularly around data bias concerning protected characteristics, underrepresented groups or the treatment of vulnerable customers.
- Technical Failures: Like any technology, AI systems can malfunction or be vulnerable to cyberattacks, leading to potential financial losses, regulatory discipline or reputational damage. Cyber security systems should be revisited to assess AI cyber vulnerabilities and mitigation.

What is the regulatory landscape around AI?

In October 2022, The Bank of England (including the PRA) and the FCA published a Discussion Paper (DP5/22) requesting feedback on how the regulator can facilitate the safe and responsible adoption of AI in UK Financial Services. This was published in response to the AI Public-Private Forum (AIPPF) final report, which made clear that the private sector wants the regulator to have a role in supporting the safe adoption of AI in UK financial services.

On 26 October 2023, the FCA and PRA published the feedback statement (FS2/23) which outlined the key responses to DP5/22. The Discussion Paper was published to initiate a debate about the risks of AI and how regulators could respond. Some of the key themes from the feedback include:

- Respondents felt the current regulatory landscape on AI is fragmented and complex, and thus a synchronised approach and alignment amongst domestic and international regulators would be particularly helpful.
- Many participants emphasized the need for more uniformity, especially when tackling data concerns like fairness, bias, and the management of protected characteristics.

Artificial Intelligence: Opportunity, risk, and regulation in financial services

- Regulatory and supervisory attention should prioritise consumer outcomes, with a particular emphasis on ensuring fair and ethical outcomes.
- Respondents noted that existing firm governance structures (and regulatory frameworks such as the Senior Managers and Certification Regime (SM&CR)) may be sufficient to address AI risks.

Looking ahead, the regulator is expected to produce further guidance by the end of March 2024.

Other considerations for firms

The use of AI in any sector carries significant ethical considerations, though these are especially pronounced within financial services.

Transparency and Data Privacy

A recent article by the ICAEW explored the ethics around data privacy and consent in relation to AI. It highlighted the existing use of AI-based insurance risk assessments in dynamic pricing, based on customer responses to health questionnaires.

However, the need to mitigate threats to customer outcomes is critical, especially within the insurance sector where dynamic pricing models can reflect bias or data leaks.

Therefore, transparency in AI, including the ability to delve into an AI model and understand its decision-making process, is crucial in building trust. This can enable consumers to better understand and challenge decisions and outcomes.

However, as it stands for many AI models (including ChatGPT), transparency is weak, leading to the current ‘black box’ paradigm, whereby systems are viewed in terms of inputs and outputs, without sufficient knowledge of internal workings and methodology.

Bias, discrimination and ESG

AI models trained on historical data can inadvertently perpetuate or amplify existing biases (see our previous article on algorithmic bias and discrimination). AI credit scoring or pricing systems might disadvantage certain demographic groups if past data reflects biases against them. This has the potential to directly contradict firms’ efforts towards promoting Diversity, Equity and Inclusion (DEI), where cognitive, conscious, and unconscious biases affect the training data.

In a best-case scenario, where underlying data is sufficiently free of bias, there is an opportunity for AI to enable organisations to understand inequalities and reduce bias in decision making. AI can be used to better monitor, and help reduce, greenhouse gas emissions, for instance by optimising energy generation and consumption across commercial premises.

Job Displacement

Automation through AI could reduce the demand for certain roles as technology may be able to replicate these activities, particularly for more junior roles performing manual tasks. The ethical considerations related to this include the societal implications of displacement, the responsibility of firms to their employees, and the impact on recruitment, staff development, talent management, and succession planning. Conversely, however, initial estimates by the World Economic Forum suggest that whilst AI could eliminate over 80 million roles, it could create almost 100 million new ones, thus the net effect appears positive.

What’s next?

It is evident that the role of AI will continue to grow, offering clear opportunities for firms to innovate, streamline processes, and amplify their competitive edge, amongst many others.

As firms look to keep up with the competition in the race to deploy AI solutions, there are a number of significant risks that firms will need to manage, which if unchecked could lead to enhanced regulatory scrutiny, litigation, fines and reputational damage. Therefore, establishing the right control environment and governance arrangements early is fundamental to manage the risks to AI.

What should Internal Audit teams think about?

AI could present both opportunities but also serious risks for firms, particularly where models are implemented unchecked and without due consideration of the risks involved. There are a number of key governance and risk management considerations for firms, including:

- There should be a documented process for the review and testing of the AI technology in use.
- Firms should consider the appropriateness of, and enhance where relevant, their governance and oversight arrangements in relation to AI.
- Senior leadership and the Board should consider and understand the relevant risks of the use of AI in the Firm, alongside their roles and responsibilities in regard to the oversight of AI.
- There should be sign-off for technology at a senior level; ensuring that senior leadership understands both the opportunities and risks of the technology and proposed control framework, promoting informed decision making.
- Another crucial factor that firms should consider, is the effect of AI on customer outcomes and its role in delivering good customer outcomes. As such, firms should commit to the ongoing review and measurement of the impact on customer outcomes and any potential unintended consequences resulting from AI.

04

ESG Update

ADAM SOILLEUX
Director

adam.soilleux@bdo.co.uk

GLORIA PEREZ TORRES
Associate Director

gloria.pereztorres@bdo.co.uk

The FCA's new anti-greenwashing rule: What is it and what steps do you need to take to be ready?

Background

The FCA's Sustainability Disclosure Requirements and Labelling Regime ("SDR") published on 28 November 2023 is introducing an "anti-greenwashing" rule. Applicable to all FCA-regulated firms, it will require firms to ensure that all sustainability-related claims are clear, fair and not misleading. In addition, any reference to the sustainability characteristics of a product or service must be consistent with the sustainability characteristics of the product or service itself.

The FCA's objective of introducing the anti-greenwashing rule, as per 4.3.1R of their ESG sourcebook, is that it will help to protect consumers from greenwashing while also creating a level playing field for firms offering products and services with genuine sustainable characteristics.

The anti-greenwashing rule was originally proposed to come into effect on the date of the policy statement, however, it was pushed back and will now only be effective from 31 May 2024.

In order to support firms with the implementation of the rule, the FCA published a Guidance consultation paper ("GC 23/3") which is being consulted on until 26 January 2024 with the final guidance expected before the 31 May 2024 implementation date.

What are the FCA's expectations around the anti-greenwashing rule

Under the proposed GC 23/3, firms will need to ensure that their sustainability related claims are:

- Correct and capable of being substantiated;
- Clear and presented in a way that can be understood;
- Complete – they should not omit or hide important information and should consider the full lifecycle of the product or service; and
- Fair and meaningful in relation to any comparisons to other products or services.

In addition, firms are required to consider the guidance in the context of the Consumer Duty and ensure that they deliver good outcomes for customers.

Ultimately, firms should be able to demonstrate that they are acting in good faith towards their customers, providing them with the information they need, at the right time, and in a clear manner whilst supporting them to pursue their financial objectives.

The FCA's new anti-greenwashing rule: What is it and what steps do you need to take to be ready?

Practical steps to consider

There is a short window in which to prepare for the anti-greenwashing rule before it becomes effective at the end of May. Whilst the final guidance, when published, may change, firms should already be starting to prepare to meet the new requirements. The following three practical steps can help firms to get ready:

Assess if the firm is making any sustainability related statements in relation to its products, services, or business strategy.

This applies to any customer facing communications or marketing materials that refer to environmental and/or social characteristics of products and services, or about how the firm does its business. In making this assessment, firms should consider communications on the website, annual and financial statements, strategies, policies, and reports.

In addition, as the rule brings into scope images, logos and colours, their use should also be assessed. According to the FCA, claims may be undermined if what they say is factually correct, but their visual presentation conveys a different impression.

Assess if all communications and marketing materials, offering documents and regulatory disclosures are accurate and consistent with the sustainability characteristics of products and services.

Firms need to ensure that communications are factually correct. The sustainability or positive social and/or environmental impact of a product or service should not be exaggerated, and any claims should be correct, coherent and consistent across all communications.

Furthermore, it is important that there is a consistent approach across the business around the meaning of the sustainability terms used to avoid inconsistencies, incoherent or incorrect claims.

Review whether there are appropriate governance and oversight controls over the sustainability communications that the firm makes.

Firms should ensure that there are appropriate oversight and sign-off processes. In addition, greenwashing risk must be regularly monitored against sustainability reference and claims. Firms should ensure that there is available evidence to support claims made. There should be a process in place to review financial promotions and other communications periodically to monitor and ensure their ongoing compliance with the anti-greenwashing rule.

What should Internal Audit teams think about?

Internal Audit teams can use the three practical steps, noted above, to support their firms in preparing for the anti-greenwashing rule. By introducing the anti-greenwashing rule, the FCA is sending a clear message to firms that it intends to challenge them over the firm's sustainability-related communications.

05

Data Protection Update

CHRISTOPHER BEVERIDGE
Managing Director of Privacy & Data Protection

christopher.beveridge@bdo.co.uk

UK Data Protection and Digital Information Bill: What is Changing for UK Firms?

Introduction

The Data Protection and Digital Information Bill was introduced to the UK Parliament in March 2023, marking a significant shift in the UK's approach to data protection and a move away from the EU GDPR. Following its second reading in the House of Lords on 19 December 2023, the draft Bill is now in the House of Lords Committee stage and anticipated to achieve Royal Assent before the next general election.

The Bill is viewed by the UK government as a strategic opportunity to create a new UK data rights regime, balancing technological innovation with robust data protection standards, and aims to alleviate the regulatory burdens on businesses, particularly small and medium-sized enterprises (SMEs).

The draft Bill introduces minor changes to the key concepts and data protection principles outlined in the current UK GDPR. It is worth noting that the UK cannot deviate too greatly from the EU GDPR or could risk losing 'adequacy status', which currently permits the free flow of personal data from the EU to the UK.

Furthermore, the draft Bill does not exempt firms from complying with other international data protection laws. For example, firms processing personal data concerning individuals based in the EU will still need to comply with the requirements of the EU General Data Protection Regulation (EU GDPR).

What does this mean for firms in the financial services sector?

The following represents some of the key changes outlined in the draft Bill which financial services firms need to be aware of:

- **Record of Processing Activities (also known as a 'RoPA'):** One of the key areas of reform within the draft Bill is a 'loosening' of the requirement of controllers and processors to maintain a Record of Processing Activities, which has historically been onerous for organisations, unless they are carrying out high-risk data processing activities. However, the draft Bill has not defined criteria for what constitutes 'high-risk' data processing although the Information Commissioner's Office is expected to publish guidance on this. Furthermore, any organisations which process personal data regarding individuals based in the EU will still be expected to comply with the requirements of the EU GDPR, and therefore will need to maintain a RoPA.
- **"Vexatious" or "Excessive" Subject Access Requests (SARs):** The draft Bill amends the criteria for managing SARs under the UK GDPR, which can also be incredibly onerous for organisations who receive a large volume of requests. The terms "manifestly unfounded" or "excessive" are replaced with "vexatious" or "excessive". This change provides explanations and guidance regarding what constitutes a vexatious or excessive request, to clarify the grounds on which organisations can refuse or limit their response to SARs.
- **Complaints management:** The draft Bill introduces the requirement for data controllers to acknowledge complaints from data subjects within 30 days and provide a substantive response promptly. The Information Commissioner's Office will not be obligated to accept a complaint if the data subject hasn't first approached the data controller.

UK Data Protection and Digital Information Bill: What is Changing for UK Firms?

- **Data protection impact assessment (DPIA):** The draft Bill proposes a transition from the prescriptive requirement to complete DPIAs to a system of "Assessments of High-Risk Processing," which is expected to simplify the process. The draft Bill removes the specific list of circumstances where a DPIA is required, and instead will rely on guidance from the Information Commissioners Office about which data processing activities require a DPIA. Furthermore, the requirement to consult the Information Commissioners Office in the event of high-risk data processing will become optional under the draft Bill.
- **Changes to the Privacy and Electronic Communications Regulation (PECR):** Changes to the PECR include allowing the use of cookies without consent for web analytics and automatic software updates. The fines under PECR will also be increased to align with UK GDPR levels, up to £17.5 million or 4% of global annual turnover, whichever is higher.

Case Study - Recent ICO enforcement action in the financial services sector

In December 2023, the Information Commissioner's Office issued a reprimand to a mid-tier bank for mistakes made on more than 3,000 customers' credit profiles. The investigation, (originally reported to the Information Commissioner's Office in 2021) found that the Bank of Ireland UK sent incorrect outstanding balances on 3,284 customers' loan accounts to credit reference agencies. Since credit reference agencies help lenders to decide whether to approve financial products, the error meant that the inaccurate data could have led to affected customers being unfairly refused credit (i.e., for mortgages, credit cards or loans), or granted too much credit for financial products that they potentially could not afford. The Information Commissioners Office investigation determined that due the to the complex nature of the impact of the error, and different factors which contribute to credit scoring, it would be impossible to quantify the impact on each customer affected but found that the Bank of Ireland UK was in breach of data protection law by failing to ensure that personal data was accurate (per Article 5(1)(d) of the UK GDPR).

To avoid some of the pitfalls highlighted in the case study, above, internal audit teams within FS firms should provide assurance that the personal data processed by First Line teams is accurate and up to date. This means considering the robustness of the Second Line processes currently in place to oversee that accurate data is captured and maintained on an on-going basis. Audit reviews on this subject should also include testing of the processes for individuals wishing to exercise their right to rectification, i.e., the right to have any inaccurate personal data corrected, and how this feeds back into the data management process of the firm. Corollary to this is the Consumer Duty's expectations for how firms support customers, especially vulnerable customers, with up-to-date information regarding their customers' circumstances when the customer has made effort to provide clarification.

What should internal audit teams think about?

The draft Bill heralds a significant shift in the data protection landscape for UK businesses and is poised to reshape how personal data is processed, offering potential benefits such as reduced regulatory burdens.

For firms which are broadly compliant with the requirements of the UK Data Protection Act 2018 and EU GDPR, the proposed changes should have minimal impact, since the draft Bill marks a 'loosening' of existing requirements of current data protection regulation. However, firms should continue to monitor the passage of the draft Bill and closely follow Information Commissioners Office guidance for greater clarity on key definitions, on revised concepts like "Vexatious" or "Excessive" Subject Access Requests. Our recent case study, below, illustrates the importance of tracking ICO requirements and guidance.

06

Tax Update - R&D

CARRIE RUTLAND
Partner

carrie.rutland@bdo.co.uk

All change for R&D tax relief in 2024: Are you ready?

The government's project of reforming UK Research and Development (R&D) relief has meant ongoing changes in recent years, and the goalposts will continue to move in 2024. Depending on the size of your firm, its profitability, the R&D costs you incur, and even when your accounting period ends, there will be many changes to watch out for if you want to understand the impact on your bottom line.

How will moving to the new merged R&D scheme affect your business?

For accounting periods starting on or after April 2024, the SME and R&D Expenditure Credit (RDEC) schemes will be merged, although for start-ups the separate scheme for R&D-intensive loss-making SMEs will continue to run in parallel. This means a significant change in the rules for current users of both schemes.

How the merged relief will work

The merged scheme will broadly follow the current RDEC rules, so the relief will be given as a taxable above-the-line credit. This will mean significant changes for SMEs in how the relief affects their accounts, and it may well be worth modelling what wider knock-on effects this could have on accounting metrics. SMEs moving to the merged scheme will also need to get to grips with the seven-step process for calculating the relief if they are seeking to model future cashflows.

However, current RDEC claimants will also benefit from modelling the impact of the fundamental changes on their R&D claims and cashflow, not least in relation to the new rules on overseas and subcontracted costs.

Costs in and out

The range of qualifying costs expanded for costs incurred on or after 1 April 2023: costs for use of datasets and cloud computing in R&D projects, as well as the cost of pure maths research (i.e. mathematical modelling, quant analysis and actuarial science), can now qualify.

However, a more significant change is coming: under the merged scheme, in the majority of cases, costs for R&D work delivered through overseas third parties or group companies will no longer qualify. Although this change was proposed some time ago, its implementation will be a major issue for many businesses carrying out R&D in the payments sector.

There will be winners and losers as a result of the new rules setting out which party can claim R&D relief when projects are contracted-out to a third party. Currently, SMEs have more opportunity to claim R&D relief in situations where R&D is contracted out, as a firm claiming under RDEC can only claim in very specific/rare circumstances.

Under the merged scheme, all principal companies may be able to claim where R&D is contracted out to a third party, provided that a 'competent professional' at the principal company specifies the terms and technical requirements of the R&D project. This can apply even where there is a chain of subcontractors, provided certain conditions are met.

In practice, this will mean that firms contracting out R&D work or acting as a subcontractor will need to factor R&D claims into contract negotiation and document their processes and contract arrangements in detail to ensure that they can make a claim. This could be a particular issue for companies that white-label their technology solutions.

Rate of relief changes

The post-tax rate of relief for the merged scheme will continue at current RDEC rates and, therefore, depends on a company's taxable profits and the corporation tax rate applied to those profits. The net RDEC at the main rate of corporation tax (25%) will be 15%, while for the small companies' rate (19%) it will be 16.2%, and for companies paying tax in the marginal rate band (26.5%) it will be 14.7%.

Although this is not a change for companies currently claiming RDEC, for most SMEs this will mean a further cut in the rate of tax relief that they receive: currently, profitable companies get an effective rate of relief of 21.5%, with loss making companies getting 26.97% if they qualify as R&D-intensive or 18.6% if not).

Making your R&D claim in 2024

Beyond the changes the merged scheme will bring, it is important to remember that the process for making R&D claims is now more prescribed than for claims you may have made before 8 August 2023. As well as providing much more specific information on the Additional Information Form (AIF) that must now be submitted with an R&D claim, in October 2023 HMRC issued new "Guidelines for compliance" setting out 13 expectations of claimants that it says should be met before a claim is submitted. Even if you pass all these tests, if you haven't claimed R&D relief before (or in the past three years) your claim will not succeed if you have failed to formally notify HMRC of your intention to make a claim within six months of the end of the relevant accounting period.

We have already seen HMRC refuse claims that are not accompanied by an AIF and expect, over time, that the Guidelines for compliance will be enforced more rigorously as well. If you want to be certain of your R&D claim and the tax relief it will generate, it is no longer cost-effective to treat it as an after-the-event exercise - data and documentation collection should really start as soon as the R&D project is conceived.

All change for R&D tax relief in 2024: Are you ready?

What should Internal Audit teams think about?

R&D tax relief will continue to provide important support to financial services businesses as they innovate and build new technology to enhance their service to customers.

For Heads of Internal Audit in firms with significant research and development activities, there should be discussion with the CFO / financial controller to check that the finance team is keeping pace with R&D tax relief developments.

Now is the time to take a fresh look at how you manage both your R&D projects and how your R&D claims are compiled to ensure that you continue to benefit – you can be sure HMRC will be doing the same!

BDO webinars: Merged R&D scheme

We are also running dedicated webinars to examine how different size businesses will be affected:

SMEs - Register for our 21 February event here

Large businesses - register for our 22 February event here

07

Economic Crime Update

JONATHAN WELLS
Manager

jonathan.wells@bdo.co.uk

Economic Crime Update

Domestic PEPs and the firm's risk assessment

On 10 January 2024 the Money Laundering and Terrorist Financing (Amendment) Regulations 2023 ("Amending Regulations") came into force.

The Amending Regulations provide changes to the enhanced due diligence ("EDD") requirements in relation to domestic PEPs (i.e., a politically exposed person entrusted with prominent public functions by the UK).

Specifically, the Amending Regulations amend regulation 35 of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 ("MLRs") to require that the 'starting point' of any assessment of the risk posed by a domestic PEP is that they pose a lower risk than a foreign PEP.

The new amendment to regulation 35(3A) will provide that:

"For the purpose of [a firm's] assessment [of the level of risk associate with the customer, under reg.35(3)], where a customer or potential customer is a domestic PEP, or a family member or known close associate of a domestic PEP -

- (a) the starting point for the assessment is that the customer or potential customer presents a lower level of risk than a non-domestic PEP, and
- (b) if no enhanced risk factors are present, the extent of enhanced customer due diligence measures to be applied in relation to that customer or potential customer is less than the extent to be applied in the case of a non-domestic PEP".

The Amending Regulations will formalise into law the approach envisaged by the FCA's Finalised Guidance FG 17/6 by requiring a differentiated approach to the extent of EDD applied in relation to lower and higher risk PEPs, with domestic PEPs being rebuttably presumed to be lower risk.

What should Internal Audit teams think about?

Whilst it is likely that most firms will already have been applying this risk-based standard to domestic PEP risk (in light of Final Guidance 17/6), the Amending Regulations now embed it into legislation, meaning that firms should be alive to the changes made, as the onus of complying with regulatory requirements is much greater. Those firms who apply the same level of EDD to all PEPs will require early consideration as they may expose themselves to public scrutiny and unwanted reputational risk by performing "too much" EDD on domestic PEP clients. To ensure a sufficient risk-based approach to EDD based on PEP risks, firms should consider:

- accurately applying the definition of PEPs – are the individuals being treated as PEPs holders of roles which are really senior enough to be PEPs?;
- conducting proportionate risk assessments of UK PEPs, their family members ("FM"), and known close associates ("KCA");
- applying EDD and ongoing monitoring proportionately and in line with risk. For example, whilst Regulation 35(5) illustrates that adequate measures should be taken to establish the source of wealth and source of funds of PEP customers, as part of its risk-based EDD, a firm may choose (as noted in FG 17/6) to apply less intrusive measures (such as only using information which is publicly available) or more intrusive measures (such as requesting independent supporting documentation) in line with the risk of the PEP; and
- keeping their PEP controls under review to ensure they remain appropriate – including how senior management are informed about and oversee operation of PEP controls.

For firms who do distinguish between lower risk PEPs and higher risk PEPs, they will need to consider if the changes to the Amending Regulations have an impact on the way in which PEP risk distinctions are drawn. This may include:

- Does the assessment take into account whether the PEP is a domestic as opposed to a foreign PEP?
- Before a domestic PEP is treated as lower risk, is there a sufficiently holistic risk assessment to ensure that there are no other relevant risk factors present? Such risk factors can include (but are not limited to) -
  - the prominent public functions the PEP holds
  - the nature of the proposed business relationship
  - the potential for the product to be misused for the purposes of corruption
  - any other relevant factors the firm has considered in its risk assessment

European Council strikes a deal on stricter AML rules

The 'Anti Money Laundering Authority'

On 20 July 2021, the European Commission presented its package of legislative proposals to strengthen the EU's rules on anti-money laundering and countering the financing of terrorism ("AML"/"CFT"). These proposals included the creation of a new agency, the Anti Money Laundering Authority ("AMLA"), which was agreed in principle by the EU Parliament and Council of the EU on 13 December 2023. The initial scope of the AMLA's tasks consisted of five broad areas, namely:

- Direct supervision of selected "obliged entities" to ensure group-wide compliance with AML/CTF requirements;
- Supervision of financial sector supervisors to ensure that all supervisors have sufficient resources and powers necessary to perform their tasks;
- Enhancing the supervision of non-financial sector supervisors;
- Financial Intelligence Unit ("FIU") coordination; and
- Rulemaking and guidance.

Economic Crime Update

The EU's AML Package

As of 18 January 2024, the Council and Parliament came to a provisional agreement on parts of the AML package. The agreed legislation will contribute to the establishment of an EU single rulebook, prevent disparities between Member States, as well as a lack of enforcement, and will provide with directly applicable European rules to ensure common fight against criminal activity.

The provisional agreement expands the list of "obliged entities" to include new bodies. The new rules will engage most of the crypto sector through requiring all crypto-asset service providers ("CASPs") to conduct due diligence on their customers. CASPs will need to apply customer due diligence measures when carrying out transactions amounting to EUR1,000 or more.

Other sectors concerned by customer due diligence and reporting obligations will be traders of luxury goods, as well as professional football clubs and agents. The Council and European Parliament also introduce specific EDD measures for cross border relationships for CASPs. These include requiring credit and financial institutions to undertake EDD measures in business relationships with high-net-worth individuals. Additionally, the agreement will see the establishment of an EU-wide maximum limit of EUR10,000 for cash payments.

The provisional agreement also makes the rules on beneficial ownership more harmonised and transparent. The agreement clarifies that beneficial ownership is based on two components – ownership and control. Both aspects need to be assessed to identify all the beneficial owners of that legal entity or across types of entity. Accordingly, the agreement previously indicated that it would consider lower beneficial ownership thresholds below 25%; however, the current proposal will see a standardised threshold of 25% across the EU. The related rules applicable to multi-layered ownership and control structures are also clarified to ensure hiding behind multiple layers of ownership of companies will become ineffective.

The European Commission's provisional agreement also expands the power of financial intelligence units ("FIUs") in analysing and detecting money laundering and terrorist financing cases. To increase transparency, FIUs will have immediate and direct access to financial, administrative and law enforcement information. The agreement emphasises that applying fundamental rights is an integral part of FIUs' work and as such, it outlines a framework for suspending or withholding consent to a transaction.

What should Internal Audit teams think about?

While the new EU AML package is not directly applicable to the UK, firms with operations in Europe should anticipate stricter AML regulatory standards and more intensive supervision as the new EU AML regime is introduced.

However, many of the details of the proposed EU AML package are, under the EU's original proposals, dependent on further technical standards and guidance to be prepared by the AMLA and will, therefore, only be available once the AMLA becomes operational.

As such, there may be some further delay until the full detail of the enhanced regulatory standards become available for firms to consider against their existing controls.

Additionally, the UK Government also seeks to be internationally perceived as "top of the class" in terms of financial crime prevention regulation, so it would be expected that the UK may look to any amendments implemented by the EU as an opportunity to enhance its own domestic regulatory landscape.

08

Motor Finance Complaints

ALISON BARKER
Special Adviser

alison.barker@bdo.co.uk

Motor Finance Complaints

You may have seen in the press that FCA is reviewing motor finance complaints about discretionary commission, sold before 2021. This is potentially a very significant issue for the industry. This article sets out the issue, FCA actions and potential timelines that internal audit teams should be thinking about.

What's the issue?

There has been a significant rise in consumer complaints about commission paid on motor finance. The Financial Ombudsman Service has about 10,000 complaints and there are reportedly many complaints going through the court system. Recent FOS and court judgements have found in favour of consumers. The FCA estimates motor finance firms have rejected about 30,000 customer complaints. Complaints are being fuelled by Claims Management Companies.

The complaints are about commission charged on motor finance (not car hire). Prior to January 2021, motor finance brokers/dealers and lenders could have discretionary commission arrangements in place. These allowed the broker/motor dealer to determine the amount of interest the customer paid on the finance, and in turn receive a higher level of commission. This should have been disclosed to the customer. These practices were banned in January 2021. Therefore, this does not apply to motor finance sold after 29 January 2021. The scope extends to motor finance sold under a discretionary commission agreement from 6 April 2014 which is the date the Financial Ombudsman Service included consumer credit in its scope.

The FCA fears there will be a disorderly process if resolution of these issues takes place through the complaints or court process, therefore they are proposing that there should be an industrywide complaint or redress scheme put in place. Their hypothesis is that customers were sold discretionary commission unfairly, contrary to the rules in place at the time and are therefore potentially owed redress.

Their current view is that the 30,000 complaints rejected may have been closed incorrectly by firms, and that many more customers may come forward to complain and firms will continue to reject the complaints.

What is happening?

The FCA recently issued a Policy Statement setting out a course of action. Their proposal is to introduce an industrywide remediation or redress programme if the evidence deems this is a widespread issue. The bar to do this is high and could take several different forms. However, to progress to a decision on the nature of the programme they have:

- Temporarily paused complaints rules to investigate and respond to complainants about discretionary commission motor finance complaints, meaning these do not have to be resolved until 25 September 2024.
- During this period, FCA will be conducting diagnostic supervisory work on a sample of firms to understand if there has been a widespread failure to follow relevant regulatory requirements at the time, numbers of customers, potential amount of redress and numbers of customers' potentially due redress.
- FCA has used powers under s.166 FSMA to commission a skilled person report to carry out the diagnostic work The sample of firms has already been selected and firms in the sample been informed. They may extend the sample to more firms.
- FCA plan to make a decision whether the issues are widespread or not, and the basis for carrying out some form of remediation exercise. If they consider a redress programme is needed, they would need to issue a public consultation. They expect to announce next steps by 25 September this year.

Motor Finance Complaints

Complaint handling – discretionary commission complaints

- The normal 8-week complaint investigation and response period is paused until 25 September 2024 for these complaints whilst the FCA completes its diagnostic and supervisory work and makes decisions on the way forward.
- Other complaints about motor finance continue to be subject to normal complaint handling requirements. Non-discretionary agreement commission related motor finance complaints to be resolved as normal.
- However, firms can expect to see a large volume of customers logging complaints now to make sure they are within any potential industrywide redress programme. Therefore, they need to be logging complaints and informing these customers that decisions are subject to a suspension for the moment.
- Firms should update websites and other customer information and communications.
- FCA is encouraging firms to continue gathering information to enable an investigation about the complaint to be completed.
- Consumer complaints could be received by either the lender, credit broker or both.

What should Internal Audit teams think about?

In advance of the outcome of FCA's supervisory and diagnostic work, Internal Audit teams should consider, either directly or in co-ordination with Second Line teams, gathering the following information:

- Understanding the potential population of consumers who could have been sold discretionary commission-based car finance between 6 April 2014 and 28 January 2021.
- Understand the number of complaints already received and upheld or rejected.
- Understanding the quality of any documentation relating to the period, for example contracts with suppliers, distributors or lenders, consumer documentation, sales processes.
- Understand how changes to complaints rules and consumer correspondence have been implemented and meet FCA requirements.
- Plan for receiving increased volumes of customer enquiries or complaints and adjustments to ensure the correct response is provided to consumers.
- Firms may have PII cover available and should contact their insurer. PII insurance can become invalid is certain circumstances, for example failure to notify or reaching a compromise with a customer.
- Consider whether appropriate notifications are made to FCA about any corporate restructures.

This is an evolving situation, and one that IA teams should raise as a potential horizon risk for senior management and Board members if the firm has exposure to motor finance.

FOR MORE INFORMATION:

Richard Weighell

+44 (0)7773 392 799
richard.weighell@bdo.co.uk

www.bdo.co.uk

XXXXXXX