IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

May 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.

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

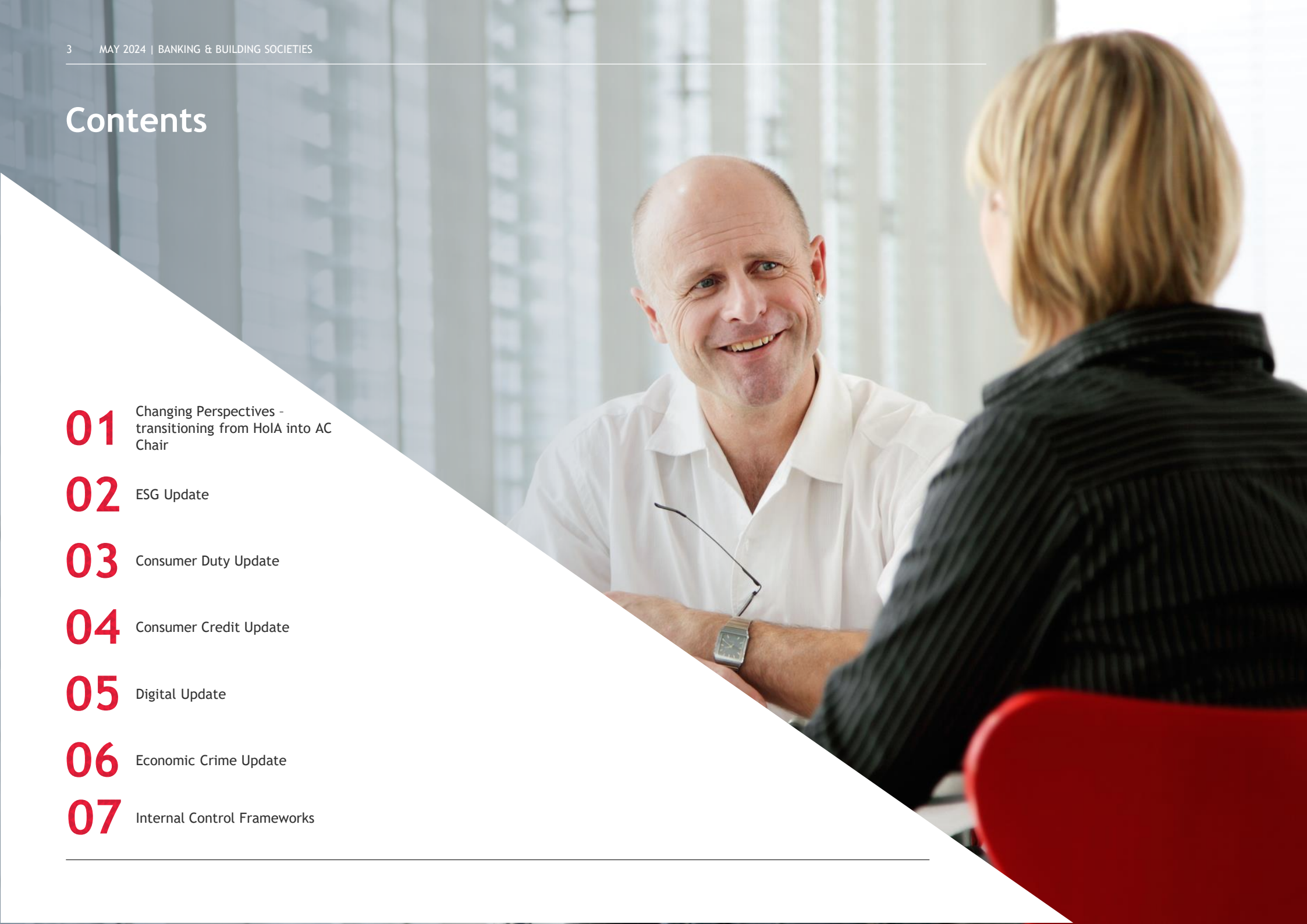
SAM PATEL
Partner

+44 (0)7970 807 550
sam.patel@bdo.co.uk

BRUK WOLDEGABREIL
Associate Director

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

Contents



01

Changing Perspectives

RICHARD WEIGHELL
Partner

richard.weighell@bdo.co.uk

Changing Perspectives: transitioning from a Head of Internal Audit into an Audit Committee Chair

At the start of July, I will be hanging up my internal audit tools and leaving professional practice after a very long time undertaking head of internal audit roles and, even longer, carrying out internal audits. However, I won't be walking away from internal audit completely, as in July I will be crossing the audit committee table to be reborn as an audit committee chair. Exciting times!

As is the way with me, this was not an impulsive decision and was something I have thought long and hard about. I love a lot of what I do and I think that I still have a lot to offer to FS firms despite the grey hairs. This approach allows me to keep involved, keep dealing with interesting people and situations and to keep myself challenged.

Since deciding that this was the right sort of move, I have been thinking about the delivery of the audit committee chair role and reading board and committee packs differently and observing chairs of audit committees and other NEDs in how they react, what questions they ask and how they respond, plus chatting to a number of them about what matters to them. It has left me with a good view of what I want from my internal audit. Much of this ties up with what I was striving to deliver as a head of internal audit, but there are a few areas where my emphasis has changed. I thought it might be worth sharing three of these with you as maybe some of these will resonate with your audit committee chairs.

First, I have always been of the view that the individual project reports are only a part of the internal audit value and just as much comes from that objective perspective of how well the business is operating overall, managing risk and preparing for the future. That view hasn't changed, but the more I have reflected on it, the more I want my internal audit teams to be taking broad perspectives on how my firm works and keeping me informed about how it is performing across the broad themes of culture, risk management, compliance, delivery and change. Better to have slightly fewer reviews and more investment in monitoring these areas so that I get ongoing feedback on these. Especially if the feedback I get is objectively based and honest. I know all of the feedback may not be able to be shared in the committee forum, but I want openness in private discussions.

Second, more detail is rarely providing more value. Yes, the responsible managers need to know the detail of the findings, but the last thing I want is a ten or twenty page report telling me something is broadly OK. Keep it short. Be clear of the scope. Be clear in the conclusions and why you reached them. Give a view on root causes. And be clear if the actions and their timescales are appropriate. That way I will be in a position to know if I need to intervene in any way and not bogged down in the minutiae. The only time that the greater detail is needed is if the report is going into an external domain, such as regulators, of if the report is specifically considering the activities of the board or committees.

Finally, timeliness matters. Receiving a report telling me how something was many months ago is not that helpful. If there are significant issues, escalate them promptly. Yes, please do give the chief executive a heads up before me, but I want to know as well, and even more so if management is being slow to respond. And if there are no points of significance, then still give me a heads up that there is nothing I need to be concerned about.

My change in role also means that this will be the last set of monthly updates that I will be editor for. From the June editions onwards, one of my fellow financial services internal audit partners, Sam Patel, will be stepping into this role and also my role as the technical lead for our FS internal audit work. I am sure that he will bring new energy to the publications.

That just leaves me to wish you success and enjoyment in your internal auditing and to specially thank those who have worked with me as clients or colleagues over the years. I hope you have found these monthly updates of value.

02

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 banks and building societies 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 banks and building societies 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, banks and building societies 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 Internal Audit teams think about?

Those banks and building societies 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, Internal audit teams 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.

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 banks and building societies 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 Internal Audit 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

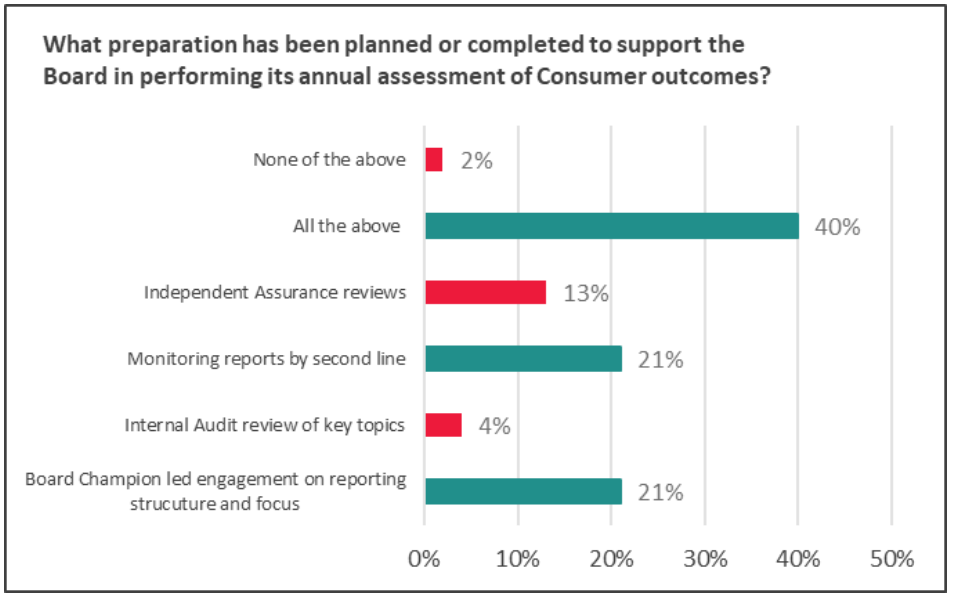
The purpose of the Board Report is to ensure banks and building societies are using meaningful MI to identify gaps and progress actions on a regular basis. The Board report enables the Board to challenge the executive on progress in delivering agreed consumer outcomes, and that organisation shifts to 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.

Banks and building societies 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 Internal Audit teams think about?

Internal Audit 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

Consumer Credit Update

ALISON BARKER
Special Adviser

alison.barker@bdo.co.uk

Consumer Credit

Consumer Credit is a fundamental part of the UK consumer market and of vital importance to consumers and retailers, as well as the banks, building societies and consumer credit firms that provide credit. Credit helps consumers smooth finances but in a challenging economic environment it can be easy for consumers to cross a line between credit as a help and credit as a burden.

The FCA estimates that 81% of UK adults hold some form of regulated credit product. In the most recent FCA Financial Lives Survey results (January 2024), results show consumers with significant challenges:

- 7.4m (14%) felt heavily burdened by their domestic bills and credit commitments
- 5.5m (11%) had missed any of these bills in the previous 6 months
- 14.6m (28%) were not coping financially or finding it difficult to cope
- 5.9m (11%) had no disposable income

This article summarises our perspective of the regulatory challenges for this market and actions that Internal Audit teams within banks, building societies and consumer credit firms can take.

Around half of the firms the FCA authorises have a credit permission, including banks, building societies, card providers, E-money services providers and other alternative finance providers. The FCA divides this large population of thousands of firms into a number of portfolios – groups of firms with similar business models.

The FCA has completed a substantial thematic review about forbearance measures for consumers in financial difficulty which finally reported in 2022. Consumer Duty implementation and Vulnerable Customer Guidance have also increased regulatory expectations of the credit sector and we are seeing increased scrutiny through skilled person reviews with a focus on creditworthiness, affordability, handling consumers in financial difficulty, complaints management and treatment of vulnerable consumers.

The FCA's most recent credit sector supervisory portfolio letter – the first one in 2024 – explains FCA's view of risks and where it will focus attention. While this most recent letter is principally aimed at High-Cost Lenders, Credit Unions and mainstream consumer credit lending providers, the critical areas within the Regulator's feedback and principles apply to the broader sector of banks and building societies. Internal audit teams within banks and building societies should consider the following areas in their planning:

Affordability

The FCA continues to emphasise that lending must be affordable. The new Consumer Duty cross cutting rule requires firms to avoid foreseeable harm to consumers, unaffordable lending is a foreseeable harm. Processes and monitoring should be in place to check lending practices remain affordable.

The recent portfolio letter also sets out expectations that consumers declined credit should be supported with sources of guidance and help.

Collections and recoveries

This area remains under considerable regulatory scrutiny. Consumers in financial difficulty may be feeling vulnerable and FCA found that 12.9 million consumers have low financial resilience and 27 million may show one or more characteristics of vulnerability. The regulatory expectation is that consumers are treated with empathy, their circumstances probed, and suitable support provided. Appropriate training, quality assurance and support for staff to manage consumer calls is vital. Call handling units need to be appropriately resourced to allow staff the time needed to handle calls well.

Price and value

High-cost lending, not subject to the High-Cost Short Term Price Cap, will be an area of focus for the FCA. The Consumer Duty imposes new requirements for products to meet fair value criteria. In other sectors, the FCA has placed considerable pressure on firms to change pricing, such as in the Wealth and General Insurance sectors. The lesson from these sectors is to ensure a robust methodology that follows the requirements set out in the Consumer Duty is applied to fair value assessments and if required, action is taken.

Complaints and redress

The FCA says it is currently reviewing complaints handling in a small number of High-Cost lenders and we can expect to see a report of their findings in due course. We are aware that some CMCs are actively probing with complaints about affordability in the credit sector. Poor complaints handling exposes firms to a range of issues including regulatory action or pressure from CMCs. The FCA requires firms to monitor complaints processes and outcomes to check whether any systemic issues should result in changes to processes.

Financial Abuse

The FCA calls out the prevalence of financial abuse where individuals may be coerced into taking out loans or credit. FCA is working with HM Treasury on this issue. However, firms need to think about how they identify and treat consumers who are victims of financial abuse including approaches to debt repayment and recording entries on credit files.

What should internal audit teams think about?

Underpinning all the above is the essential role of the three lines in assessing and monitoring risks, tracking management actions, and providing challenge where practices fall below regulatory expectations and risk tolerances. For internal audit teams within banks and building societies, common areas for assurance work include evaluating if the firm has a robust and clear governance framework, documented risks and compliance arrangements, and regular reporting to the firms' Board.

Consumer Credit

Actions that IA functions should consider:

- Look at the issues raised in the Portfolio letter and check they areas covered in first line controls and second line monitoring.
- Assess whether current outcomes MI has sufficient scope, depth and breadth or whether there are gaps in reporting.
- Evaluate whether the information you have identifies any systemic issues that require management attention.
- If there are gaps in your MI or controls, look at remediating these in a timely manner
- Check governance, risk and compliance arrangements are robust. For example, documented terms of reference for committees, a robust and comprehensive monitoring plan, documented compliance and risk policies and procedures.
- Check monitoring is completed to schedule and sufficiently resourced.
- Check risk and compliance reports and actions are tracked and closed appropriately.
- Where actions are outstanding understand why and plan to resolve.

05

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.

Regulated firms are increasingly incorporating AI/ML into their operations and 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 Internal Audit Teams think about?

Internal Audit Teams 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.

06

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 Internal Audit teams 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.

IA functions 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.

07

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 Internal Audit teams 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.

FOR MORE INFORMATION:

Richard Weighell

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

www.bdo.co.uk

XXXXXXX