IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

March 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

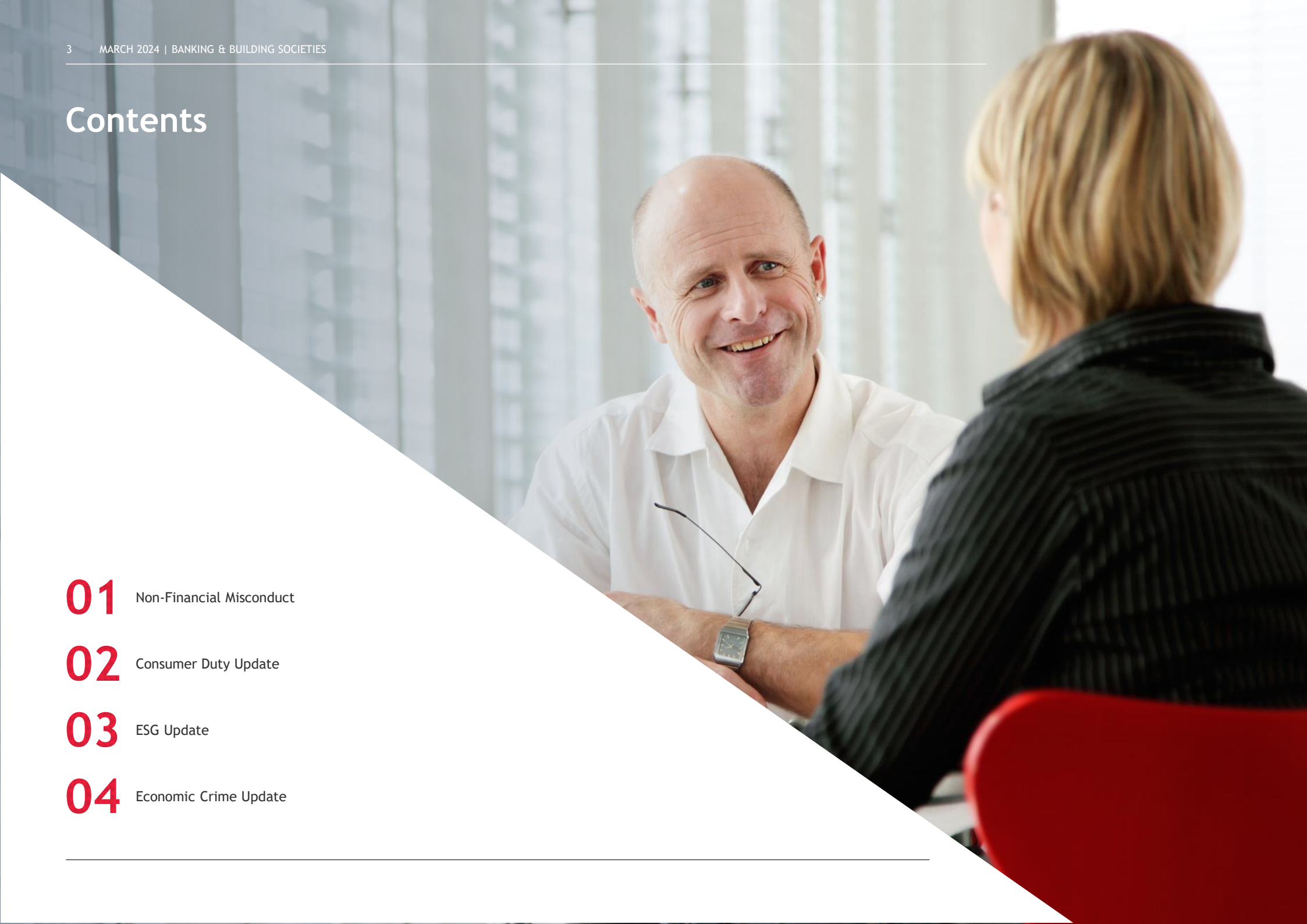
CHRIS BELLAIRS
Partner

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

BRUK WOLDEGABREIL
Associate Director

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

Contents



01

Non-Financial Misconduct

SASHA MOLODTSOV
Partner

sasha.molodtsov@bdo.co.uk

What is the FCA's Non-Financial Misconduct (NFM) survey and how does it link to the broader regulatory agenda?

The Financial Conduct Authority (FCA) recently intensified its supervisory work on Non-Financial Misconduct (NFM) by issuing a "Notice to Provide Information" to the Insurance sector (under section 165(1) of the Financial Services and Markets Act 2000 (FSMA)) related to incidents of NFM.

While targeted at the insurance sector initially, the NFM Survey signals the broader direction of regulatory travel that firms across other financial sectors should be mindful of and should ensure are on their radars.

NFM is an area that sits at the heart of the recent FCA Diversity and Inclusion (D&I) Consultation Paper and the Treasury Select Committee's Enquiry into "Sexism in the City". It demonstrates the ongoing regulatory focus on conduct, diversity, and inclusion (D&I), governance and accountability - and perhaps the golden thread linking each of these areas - culture.

The FCA is using the survey to collect data on: the volume and type of incidents of NFM, the methods of detection (e.g. whistleblowing), and the actions taken to address incidents. It has stated that the information collected will enable "a clearer understanding of when and where NFM occurs, … a baseline assessment of each sector and inform … ongoing supervisory work".

What is Non-Financial Misconduct?

The FCA describes NFM as behaviour or actions within a financial services firm that do not directly relate to the financial aspects of the firm's business but can still have a significant impact on its conduct, integrity, and reputation. This can include things like bullying, harassment, discrimination, or any other behaviour that creates a hostile or complicit work environment.

Why is the FCA concerned about NFM?

As referenced above, the FCA believes that NFM can be a measure of a firm's culture and is therefore relevant to the assessment of a firm's ability to conduct business in line with regulatory standards. A poor culture is more likely to facilitate or be complicit in enabling poor decision making and/or permitting activities that breach regulatory standards.

However, there has been some debate around whether NFM falls within the FCA's remit - and even legal challenge. For example, around whether certain behaviours (particularly outside of the workplace) do speak directly to an individual's fitness and propriety to work within the financial sector or not.

Despite this (and the clear need for robust processes that enable firms to identify and act on any allegations of NFM in a fair and appropriate way), there is a growing body of research that seemingly supports that – yes – there are established links between positive (diverse and inclusive) cultures - and outcomes (in terms of conduct, decision-making, and even innovation and commercial outcomes) – that align with the FCA's statutory objectives of protecting consumers, ensuring the integrity of the UK financial system, and promoting effective competition.

As such, the direction of travel is clear - it's not just about complying with rules - it's about embedding a culture that promotes (and incentivises) the right behaviours and is inclusive and psychologically safe (so that any issues that do arise are promptly identified and addressed).

But how do firms go about doing this?

Embedding a healthy culture

Culture is not a new topic for the FCA, and most firms will be very familiar with the FCA's four "drivers of culture": purpose, leadership, approach to rewarding and managing people, and governance. Purpose has received significant attention, being described as a firm's "reason for existing, and why the world would be worse off without the value it provides" (FCA, Marc Teasdale, Director of Wholesale Supervision). The premise being those different purposes (e.g., a customer-centric versus non-customer-centric purpose) drive different decision-making and outcomes.

However, establishing a clear purpose, values, and desired culture is one thing – ensuring that that culture has been embedded, is quite another. The UK Corporate Governance Code (2024) has even been updated to make that distinction, and it now requires boards (of listed firms) not only to assess and monitor culture but also how the desired culture has been embedded.

This is often an area firms struggle with as culture can seem intangible – and so a few points to consider:

- Firstly, do you have all the right foundations in place? Such as a defined purpose and values that are clear and well-understood. Your firm's purpose and values should be threaded through your people policies and incentivisation arrangements.
- How do you evaluate your culture? Do you have a robust framework for this – or is your firm's approach less well defined?

What is the FCA's Non-Financial Misconduct (NFM) survey and how does it link to the broader regulatory agenda?

- What role do the three lines of defence play when it comes to culture? For example, does culture feature on your compliance monitoring and internal audit plans? If not, how does your board gain assurance around whether the desired culture has been embedded?
- How do you monitor culture and what management information is used to support this? Are your metrics carefully considered and supported by analysis and insights?

The culture conversation is not one likely to ebb away, and so if you don't have clear or comforting answers to the above, it's worth confronting this head on.

Encouraging "speaking up" and fostering psychological safety

The FCA describes NFM as behaviour or actions within a financial services firm that do not directly relate to the financial aspects of the firm's business but can still have a significant impact on its conduct, integrity, and reputation. This can include things like bullying, harassment, discrimination, or any other behaviour that creates a hostile or complicit work environment.

Why is the FCA concerned about NFM?

The NFM Survey not only requests data for NFM incidents, but also the method by which the incidents were detected. Whistleblowing is of course a key mechanism for raising concerns, and firms should consider reviewing the design and effectiveness - not only of their policies - but of their end-to-end process, including:

- The channels (communication methods) in place, and the clarity/prominence of these - and training and awareness;
- The controls regarding confidentiality and ensuring there are no adverse consequences for whistleblowers;
- The assessment and escalation processes - including mitigation of conflicts of interest and the role of the whistleblower's champion; and
- Management information, reporting, and outcomes - including actions taken in relation to substantiated concerns.

Whistleblowing also won't be the most appropriate channel for all concerns, and firms should reflect on the other mechanisms they have in place to encourage employees to share their opinions and concerns.

Perhaps most importantly, there also needs to be an awareness that – without a safe and inclusive environment, people may not be/feel able to speak up, even where there are channels to do so in place. And so fostering psychological safety is key. Psychological safety in the workplace should create an environment where employees feel safe to innovate, voice their opinions, and admit mistakes. The aviation industry is often cited as an example where an open culture exits to continually improve safety by learning from flight data and incidents. Psychological safety is not just about being nice or avoiding conflict. Instead, it's about encouraging open dialogue, promoting diversity of thought, and ensuring that everyone's views are heard and respected. A psychologically safe environment can lead to better decision-making, increased innovation, and improved risk management.

As a few points to consider:

- How do you know if employees feel safe and able to speak up?
- What mechanisms do you have in place to encourage speaking up – beyond your whistleblowing channels?
- How do you monitor the effectiveness of your speak up channels and culture? And use this information to inform continuous improvements?

Enhancing diversity and inclusion

NFM is a core element of the recent FCA D&I Consultation Paper (CP23/20). The proposals include better integrating NFM considerations into fitness and propriety (F&P) assessments, the Conduct Rules, and the suitability criteria for firms to operate in the financial sector (i.e., the Threshold Conditions).

However, the crux of the focus on NFM, is about tackling poor behaviours, and particularly (but not exclusively) discriminatory behaviours, to create a safe and inclusive environment where diverse talent can thrive.

And so when you're considering the CP proposals and how your firm plans to implement these, it's worth making sure that:

- Your firm is focusing on fostering inclusion as well as diversity - this means thinking about inclusion as part of your strategy as well as inclusion metrics.
- NFM is considered, not just in the context of F&P assessments and conduct rule reporting, but in terms of the mechanisms for identifying, managing, and learning from NFM (as referenced in the section above).

What is the FCA's Non-Financial Misconduct (NFM) survey and how does it link to the broader regulatory agenda?

Ensuring effective governance

The NFM Survey also asks questions around governance and management information (MI). This is no surprise given that governance is one of the FCA's four drivers of culture. But what does good governance look like? And how does good governance promote healthy culture and conduct? Firms are required (in accordance with SYSC General requirements - 4.1.1R) to "have robust governance arrangements, which include a clear organisational structure with well defined, transparent and consistent lines of responsibility" and "effective processes to identify, manage, monitor and report the risks it is or might be exposed to." But there's more to consider here. For example:

- The composition of your board and board committees – do you have the right mixture of skills, experience, and diversity? (to provide a range of perspectives and experiences that can help to challenge groupthink and drive better decision-making).
- Board culture - Is the board and committee culture itself facilitative of effective discussion and decision-making? (e.g., is it inclusive and focused on continuous improvement).
- Board effectiveness – do you have appropriate mechanisms in place to evaluate the performance of the board and board committees? These reviews should be regular and robust (e.g., should include consideration of the above, as well as MI, decision-making and overall functioning).
- MI – does your firm have the right MI at board level and across broader governance forums? Coverage, content, quality, timeliness are all important – particularly when it comes to areas such as culture, D&I, and NFM. We have often seen limited metrics and meaningful analysis in these areas which raises the question as to how boards get comfortable that a healthy culture has been embedded.

What should Internal Audit teams think about?

- **How it all fits together**: Third line teams should consider how the firm conducts Fit & Proper assessments, regulatory references and reporting on conduct rule breaches. Typically, these activities straddle multiple teams, e.g., Risk, Compliance, HR, etc therefore it's important that the Internal Audit function has the big picture on specific accountabilities for these processes within first and second lines to provide effective assurance coverage. Co-ordination for IA's reliance on second line's assurance over some of these activities can produce efficiencies for the IA function and incorporate the input of compliance experts with specialisms not typically found in IA.
- **Culture**: The firm's overall framework for creating and embedding a healthy culture, D&I, and monitoring culture will be a critical tool for addressing NFM. Culture as a component of audits can help the IA function identify problematic behaviours early before they evolve into sub-cultures within teams.
- **Tone from the top**: Board and governance arrangements, particularly the effectiveness of the arrangements, should be considered for the annual plan if not already confirmed. IA teams should also evaluate the firm's conduct policies and procedures, including whistleblowing and other "speak up" mechanisms that feed into the governance arrangements, as well as the disciplinary processes, remuneration and incentivisation arrangements that are put out by the Board. The firm's current state of NFM risk is likely driven, in part, as an outcome of these inputs and outputs that help frame the firm's culture. Therefore, IA functions should be assessing these flows of information to understand what is feeding the NFM risk.

02

Consumer Duty Update

ALISON BARKER
Special Adviser

alison.barker@bdo.co.uk

Focus on Closed Books

Banking & Building Societies

A recent speech by Sheldon Mills, FCA Executive Director of Consumers and Markets, highlighted the Consumer Duty implementation date of 31 July 2024 for Closed Books is fast approaching.

Closed books are defined as product no longer marketed and sold. “(1) where there are existing contracts with retail customers entered into before 31 July 2023; and (2) which is not marketed or distributed to retail customers (including by way of renewal) on or after 31 July 2023. (FCA Glossary)

The speech shows the level of expectation the Regulator has over work firms should be doing to apply the Consumer Duty to legacy products and the common challenges facing firms.

Data Gaps

Unsurprisingly, records such as terms and conditions, original sales records or even policy documents, may have gaps or be missing particularly if products are decades old.

The FCA expects firms to try their best to resolve gaps, and if that is not possible put in place outcomes testing to check customers are receiving good outcomes, be that on understanding the nature of their product, its ongoing appropriateness and suitability, or helping them achieve their financial goals.

A common issue is customers who are ‘gone away’ or no longer engaged. The FCA is keen to see more efforts to contact customers, support them and help them understand the products they have. The consequence of this, would be supporting customers where products are no longer suitable for their needs.

Price and Value

A fair value assessment is required. If a firm knew about a particular issue with fair value, the expectation is that it is put right. Firms are not expected to re-price products as a matter of course or reperform underwriting.

However, this takes us to vested rights. These are defined as including:

“pre-existing contractual rights to which a firm already has legal entitlement (e.g. annual fees that are due) and rights to payments falling due on occurrence of a contractually specified event (e.g. exit charges).”

The Consumer Duty is not retrospective, however, the Regulator is encouraging firms to remove contractual rights, such as exit charges, from legacy/closed products. This starts to be a controversial area where it impacts profitability and financial assumptions based on contractually vested rights from a legacy book of business.

Focus on Closed Books

Banking & Building Societies

The time available to meet the requirements for closed books is short with only five months to go until end of July. The FCA has recognised that firms may be struggling to meet the deadlines and advise prioritisation with a focus on:

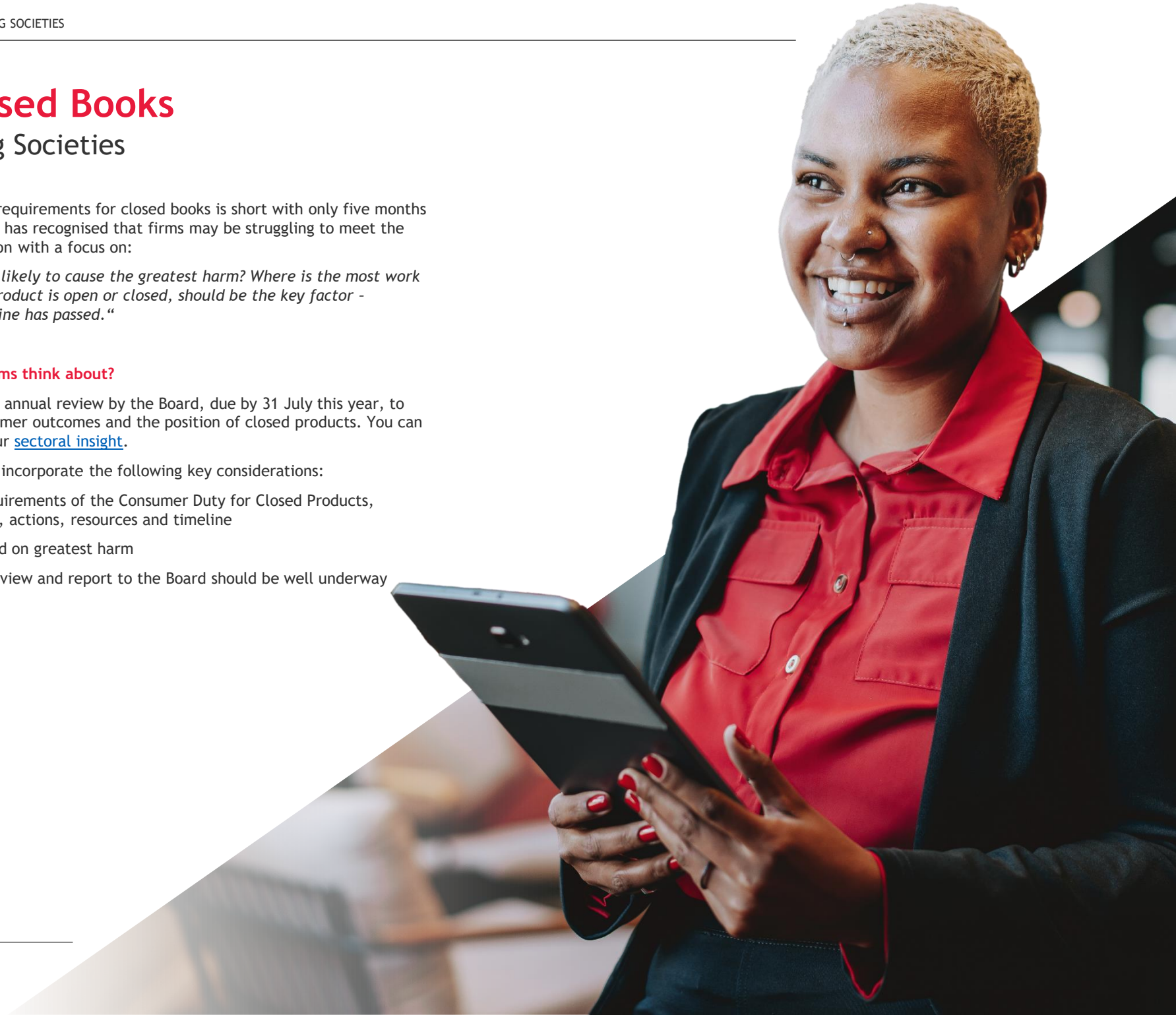
"Which products or services are likely to cause the greatest harm? Where is the most work needed? This, rather than if a product is open or closed, should be the key factor – particularly once the July deadline has passed."

What should Internal Audit teams think about?

An important requirement is the annual review by the Board, due by 31 July this year, to report on delivery of good consumer outcomes and the position of closed products. You can find out more about this from our sectoral insight.

Internal audit teams should also incorporate the following key considerations:

- A plan for delivering the requirements of the Consumer Duty for Closed Products, understanding scope, impact, actions, resources and timeline
- Prioritisation of actions based on greatest harm
- Preparation of the Annual Review and report to the Board should be well underway



03

ESG Update

ADAM SOILLEUX
Director

adam.soilleux@bdo.co.uk

GLORIA PEREZ TORRES
Associate Director

gloria.pereztorres@bdo.co.uk

Taskforce for Nature-related Financial Disclosure: Current expectations and future developments

According to the Word Economic Forum's report Future Of Nature And Business: "Nature is declining at an unprecedented rate, with nearly 1 million species at risk of extinction because of human activity". As other ESG factors continue to evolve, 'nature risk' is emerging as a critical aspect of strategic risk management. In this scenario, regulatory scrutiny, business risks and demands from stakeholders continue to increase and financial institutions are under pressure to evaluate, disclose and actively address nature-related risks.

In response to the increasing demand for nature-related risks to be factored into financial and business decisions, the Taskforce on Nature-related Financial Disclosures (TNFD) introduced a set of disclosure recommendations and guidance to encourage and enable firms to assess, report and act on their nature-related dependencies, impacts, risks and opportunities.

To support TNFD implementation in the financial sector, the Taskforce published Sector Guidance for financial institutions on how they should report on the TNFD recommendations. The Taskforce is seeking feedback on the guidance, by 29 March 2024, and while they do not intend to change its recommended disclosures, periodic updates will be published over the next two years, incorporating feedback from market participants and other stakeholders.

What is the TNFD Framework?

The TNFD is a framework of 14 recommendations on how to report on nature-related risks and opportunities. The objective behind TNFD reporting is to build data and information that can be used for decision making and supporting financial flows towards biodiversity friendly projects.

Firms will find a familiar format in the TNFD recommendations as they were designed to be consistent with the language, structure, and approach of the Task Force on Climate related Financial Disclosures (TCFD) recommendations and around the four disclosure pillars: Governance, Strategy, Risk Management and Metrics and Targets. This structure will be useful as firms may wish to consolidate both the TNFD and the TCFD within one comprehensive report.

The guidance is intended to be applied on reporting at entity-level and provides an overview of how to report on the 14 recommendations, on a comply or explain basis, providing detail by sub-sector. The guidance also includes a recommended set of TNFD disclosure metrics.

The recent TNFD consultation requested feedback from financial institutions on these proposed disclosure metrics, and the extent to which the metrics are relevant, useful and ample enough. Where possible, firms should consider the proposed metrics and comment on whether these seem appropriate and useful for financial institutions.

What should Internal Audit teams think about?

Firms engaging early will need to review and update their ESG strategies and plans to be TNFD aligned. This includes incorporating nature-related considerations into business strategies and it is recommended that these considerations are aligned with decarbonisation and/or transition plans.

Internal Audit teams, therefore, will need to provide assurance over the firm's completion of critical activities, including development of a strategy, governance, risk management and metrics and targets in relation to nature-related risks and opportunities.

Furthermore, the IA function will need to check that the first and second lines are appropriately introducing or updating internal human rights policies and engagement activities, with respect to Indigenous Peoples, Local Communities and other stakeholders who can be affected by the firm's financial activities.

TNFD is at the moment a voluntary framework. However, on 23 February 2024, the Government responded to the Environmental Audit Committee report on the financial sector and the UK's net zero transition, recommending that Ministers set out an overarching implementation timetable for mandatory TNFD reporting.

More broadly, ESG expectations keep continuing to evolve. Whether firms decide to engage with TNFD now or later, will be a business decision. However, early consideration may give firms a competitive advantage against peers.

04

Economic Crime Update

CLARINDA GRUNDY
Associate Director

clarinda.grundy@bdo.co.uk

Economic Crime Update

UK Government publishes its national sanctions strategy

On 22 February 2024 the UK Government published its national strategy setting out the UK's approach to using sanctions to address global threats and protect the home market - Deter, Disrupt and Demonstrate.

The strategy outlines how the UK uses, and intends to continue to use, "carefully-deployed" financial sanctions to address "malign activity" and make a real difference in preventing and deterring acts and harmful behaviour such as "disrupting Russia's war machine, confronting cyber gangs that target the UK and addressing human rights abuses and violations in Iran".

What should Internal Audit teams think about?

It is important to note that the publication of the UK's sanctions strategy does not symbolise a turning point in the UK sanctions agenda, nor does it bring new expectations over and above enforcing existing high standards. Internal audit teams should, therefore, continue to ensure second line teams prioritise developing and maintaining a sophisticated and agile sanctions compliance framework which enable firms to comply with current regimes as well as adapt to future amendments.

The fundamental considerations for audit planning on this subject include:

- Business wide risk assessment ('BWRA'): Identifying and assessing their business-wide sanctions risk exposure based on their size, scale, nature, customer base and business activities;
- Clear policies and procedures: Developing and implementing clear policies and procedures for sanctions compliance based on the risks identified in the BWRA and the sanctions compliance controls deployed;
- Effective screening systems: Using reliable and appropriate screening systems to identify sanctioned individuals, entities, and countries, and ensuring list management protocols are robust;
- Governance – ensuring that appropriate escalation channels are in place to take risk-based decisions on potential and true matches;
- Regular training and awareness – providing regular training to staff on sanctions compliance, how to identify potential sanctions nexuses and what next steps to take, and any relevant updates to the applicable sanctions regimes;
- Regular audits – conducting regular audits/gaining third party assurance to ensure that the firms sanctions compliance programmes are operating effectively and as expected; and
- Swift reporting and response – establishing a framework for prompt external reporting of potential sanctions breaches and taking appropriate action (e.g., account freezing).

February 2024 FATF Plenary outcomes

On 23 February 2024, the FATF publishes the outcomes of its Plenary which took place over 21-23 February. Key updates include, but are not limited to:

1. Addition of Kenya and Namibia to the list of 'Jurisdictions Under Increased Monitoring';
2. Removal of Barbados, Gibraltar, Uganda and the United Arab Emirates from the list of 'Jurisdictions Under Increased Monitoring';
3. The FATF 'High-Risk Jurisdictions subject to a Call for Action' list has not changed;
4. The FATF will soon publish updated guidance on beneficial ownership and transparency of legal arrangements. This will reflect input from public consultations on the draft guidance following the FATF'S October Plenary; and
5. The FATF intend to consult on updates to Recommendation 16 to help make cross-border payments faster, cheaper, more transparent and more inclusive whilst ensuring AML/CFT compliance.

Related to points #1, #2 and #3, above, HM Treasury has also published an Advisory Notice clarifying its stance on the application of Enhance Due Diligence ('EDD') measures to relationships involving jurisdictions identified as having strategic deficiencies in their AML/CTF regimes (i.e., FATF 'Jurisdictions Under Increased Monitoring' and 'High-Risk Jurisdictions subject to a Call for Action'). Amongst other things, this confirms that the FATF 'Jurisdictions Under Increased Monitoring' and 'High-Risk Jurisdictions subject to a Call for Action' are now considered 'High-Risk Third Countries' as defined by Regulation 33 of the UK Money Laundering Regulations.

What should Internal Audit teams think about?

With respect to updates #1, #2 and #3 above, and following recent updates to the UK AML/CFT framework, Internal Audit teams should evaluate how the second line has effectively reflected the changes to the 'High-Risk Third Countries' in their AML/CFT frameworks with respect to EDD. Firms should be preparing to update their country, customer, and business-wide risk assessment approaches, EDD procedures, governance mechanisms and training material accordingly.

Regarding update #4, above, IA should plan assurance on how the firm's control function has incorporated the FATF guidance on beneficial ownership and transparency of legal arrangements when published. This is likely to build on the existing FATF Guidance on Beneficial Ownership of Legal Persons (published in March 2023) supporting firms to use a "multi-pronged approach" to collect and verify beneficial ownership information to ultimately gain comfort that ML/TF risks are being appropriately identified and managed/mitigated.

FOR MORE INFORMATION:

Richard Weighell

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

www.bdo.co.uk

XXXXXXX