IDEAS | PEOPLE | TRUST

Internal Audit Support

Banking & Building Societies

April 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

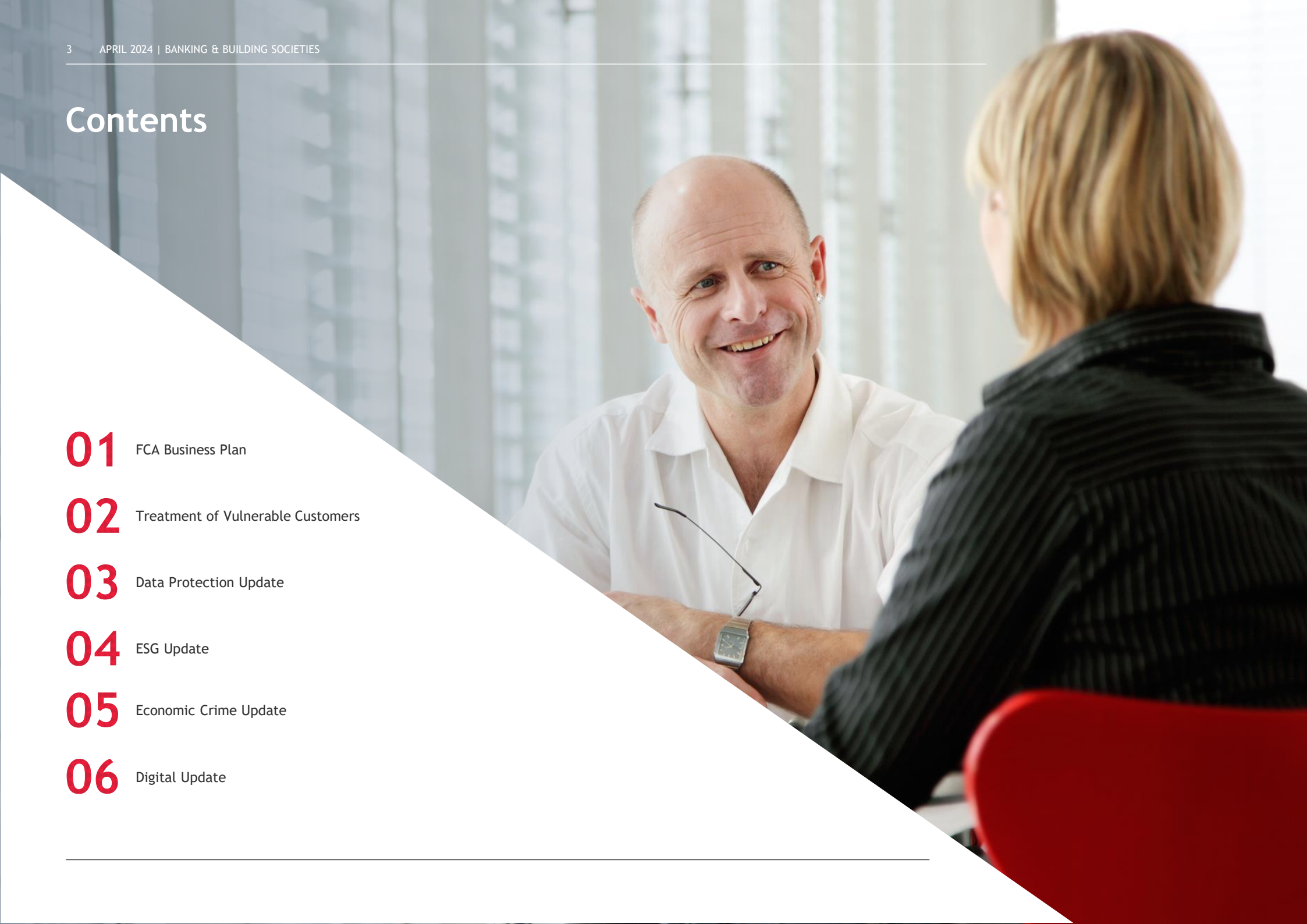
CHRIS BELLAIRS
Partner

+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

FCA Business Plan

ALISON BARKER
Special Adviser

alison.barker@bdo.co.uk

FCA Business Plan: What Should Internal Audit Think About?

The Financial Conduct Authority (FCA) published its annual business plan on 19 March. This is the third year of its three-year strategy to achieve better outcomes for consumers and markets. Having a three-year strategy has enabled the regulator to take a longer-term approach and deliver substantial policy initiatives and its own transformation agenda. This year's Business Plan is therefore a continuation of that strategy with an emphasis on assessing those outcomes.

The Consumer Duty continues to be the focus for delivering a step change in consumer protection. The regulator is committed to embedding the Duty in its supervisory agenda as well as completing the implementation for Closed Books in July this year. We can expect to see supervisory assessments continuing to focus on price and value. The FCA has already announced a review of the outcomes for vulnerable consumers.

The next significant areas are the retirement income agenda and the value for money proposals for Defined Contribution pensions. These are also a continuation of initiatives and involve working closely with the PRA and The Pensions Regulator. Ensuring consumers receive good quality retirement income advice and that pensions deliver value for money are essential steps to improve consumer outcomes in retirement. Linked to this are the challenges in resolving what is commonly called the 'Advice Gap'. The Ambition is to introduce new ways to provide more tailored information to aid investment decision making and support to consumers priced out of receiving full financial advice.

FCA's role in preventing fraud and scams also continues with the FCA playing its part in the UK's Economic Crime Plan and Fraud Strategy, both published in 2023. The FCA is shifting its operating model to being more proactive in using data and intelligence to disrupt, pursue and sanction those engaging in financial crime. The FCA will also continue its role market surveillance and taking tough action on market abuse. Further details can be found on page 14, below.

Wide ranging reforms to the UK's capital markets also continue as well as fostering growth and competition through the Sandbox initiatives. This will include finalising the review and proposals on a new Listing Regime and consulting on options for paid for research and commodities position limits.

The secondary objective on international growth and competitiveness is new and only published in July this year. It has set in train actions for the regulator to review how it will implement this although a focus on the speed and ease of authorisation will be key.

Along with the Business Plan, the FCA also published four documents that explain how it operates. These 'Our Approach' publications are short summaries about the FCA's approach to Consumers, International Firms, Supervision and Competition. They update the previous (much longer) Our Approach documents published in 2018.

The new publications set out FCA expectations and how it works at a high level as well as updating to include the Consumer Duty as its core approach to outcomes.

The explanation of FCA's Approach to Competition sets out how this operates alongside other objectives and the philosophy of the role of competition in well-functioning markets. It provides a simple explanation of the FCA's focus on price and value in consumer markets. It shows that competition is now well integrated into FCA's policy, supervisory and authorisations thinking.

The Approach to Consumers brings together several strands of potentially tricky territory: consumer responsibility, consumer vulnerability, asymmetries of information and financial inclusion. The publication sets out that FCA is responsible for addressing imbalances in information or consumer vulnerability, as well as helping consumers to make informed choices. However, it has no specific responsibility to ensure all consumers have access to financial services, only to have regard to how easy it is for consumers to access and that markets work well for consumers.

The Approach to Supervision integrates the Consumer Duty and Competition perspectives as well as articulating the FCA's more data led approach. Many firms will have experienced this over the last year with an increasing use of surveys and outlier analysis. The publication emphasises expectations of firms to focus on good consumer and market outcomes, the standards expected of firms and individuals across consumer, market, and prudential requirements.

The Approach to International Firms is aimed at those firms seeking to be authorised in the UK and provides a useful explanation of what to expect through the authorisation process. It starts with a list of firm types excluded from the Approach (Payment Services and Emoney firms and AIFs, UK Authorised funds' managers, trustees and Depositaries, and Benchmark Administrators).

02

Treatment of Vulnerable Customers

THOMAS STORY
Senior Manager

thomas.story@bdo.co.uk

The FCA's upcoming review of firms' treatment of vulnerable customers

The FCA has recently published its Business Plan for 2024/25. In it the FCA set out its areas of focus for the next 12 months. As this is the last year of its three-year strategy and an election year it was not full of surprises.

One area that will be in focus is 'protecting customers' and the embedding of the Consumer Duty regulation, the FCA has announced that it will be conducting a review of firms' treatment of vulnerable customers as one of its key activities this year and intends to share its findings by the end of 2024.

This review was foreshadowed in the FCA's 2021 guidance for firms on the fair treatment of vulnerable customers and, particularly with the implementation of the Consumer Duty, it will expect firms to have taken sufficient and appropriate action to: (1) understand their vulnerable customer population; and (2) enhance the outcomes vulnerable customers receive.

This review will look at the areas initially highlighted within the 2021 fair treatment of vulnerable customers guidance, namely:

- Firms' understanding of customer needs;
- The skills and capability of staff;
- Product and service design; and
- Communications and customer service.

It will also look at the outcomes vulnerable customers receive and how these compare to the outcomes experienced by other customers – a key subject area within the Consumer Duty regulation.

What should Internal Audit teams think about?

Many firms will have recently completed a significant programme of work to implement the Consumer Duty for existing products and services and will feel comfortable the actions taken to embed the fair treatment of vulnerable customers within their ways of working. We have seen the FCA take a tough stance on subjects it has previously cautioned firms need to take action. FCA has an increased willingness to use all the supervisory tools, including skilled person reviews, to ensure firms are clear about their expectations.

There are a set of proportionate and pragmatic steps internal audit teams should think about to ensure they are aligned with the FCA's current expectations and to prepare themselves for potential future regulatory scrutiny of treatment of vulnerable customers:

Firms' understanding of customer needs

The Consumer Duty requires firms to act to deliver good outcomes for all its customers, including vulnerable customers. To support delivering good outcomes to specifically vulnerable customers firms will need to understand the needs of those customers and the drivers of vulnerability, which are likely to vary between products and target markets.

- Review the makeup of the vulnerable customer population that hold your products or are within your product target markets – is this sufficiently detailed to see them as more than 'just a vulnerable customer'; and
- Consider the impact that different vulnerabilities and different drivers of vulnerability have on the outcomes vulnerable customers may experience and where the risks of poor outcomes may arise.

The skills and capability of staff

Staff at all levels within a firm play a role in influencing the outcomes that vulnerable customers experience. This is particularly true for customer-facing staff, who need to have a clear understanding of how their interactions with customers can materially change the overall outcome a customer can experience and be equipped with the right tools to support good outcomes.

- Ensure your customer-facing staff have received appropriate and proportionate training, based on your products and target market, on identifying and engaging with vulnerable customers and having potentially challenging conversations; and
- Encourage staff to take the time to understand customers' circumstances, for example, where they are in financial difficulty so that staff can identify the right forbearance solution appropriate to their needs and are directed to other relevant sources of help.

Product and service design

Products and services may have features that result in unintended harm and poorer outcomes for vulnerable customers. As such, firms should ensure that appropriate care and attention is given to vulnerable customers within the target market and as part of product design or review.

- Consider whether your product review processes, and the template or other tools used to complete these reviews, support you in understanding the outcomes experienced by vulnerable customers at every stage of the customer journey and product lifecycle;

The FCA's upcoming review of firms' treatment of vulnerable customers

- Revisit completed product reviews to understand if these are clear on the impact of customer vulnerability on the utilisation, benefits and limitations of the products and the differences in outcomes that may be experienced as a result.

Communications and customer service

Vulnerable customers are more likely to have different needs when interacting with firms and are at greater risk of experiencing materially poor outcomes when these needs are not met. Firms should understand what the needs of vulnerable customers within their target markets are and set themselves up to meet those needs.

- Review whether your customer engagement pathways support you in engaging with your customers flexibly and empathetically in view of their differing needs (e.g. multiple communications channels and using proactive communication to check understanding); and
- Ensure communications are appropriate to the target market and signpost where additional support may be available (e.g. third-party debt support, where the FCA has recently published a letter).

Effective outcomes monitoring

As part of acting to deliver good outcomes for customers, firms need to have a clear understanding of what 'good' looks like. Firms' monitoring should enable it to pinpoint where poor outcomes are being experienced and the root causes for those poor outcomes.

- Ensure that reporting enables management and the Board to read across outcomes between vulnerable and other customers and supports a positive discussion around the potential root causes.
- Assess whether the frequency and depth of MI and other reporting is appropriate for difference committees or working groups within the firm's governance structure.

03

Data Protection Update

CHRISTOPHER BEVERIDGE
Managing Director of Privacy & Data Protection

christopher.beveridge@bdo.co.uk

ICO Priorities moving forward

In a recent speech, the Information Commissioner, John Edwards, outlined the key priorities for the ICO over the coming months. These included:

- Advertising technologies and fair use of cookies – The Information Commissioner acknowledged the current power imbalance between online advertisers/aggregators and end users. In early 2024, the ICO reviewed the top 100 websites in the UK and identified 53 as having potentially non-compliant cookie banners. Those organisations were given 30 days to address non-compliance or potentially face enforcement action. Based on these figures, the Information Commissioner indicated that ICO time and resource will continue to focus on how to monitor and regulate cookie compliance, at scale.
- Artificial Intelligence (AI) - Given the transformative power and increased usage of AI (including within the Financial Services sector), the Information Commissioner confirmed that the ICO is focusing on ensuring that AI technologies are implemented in a way that complies with the principles of UK data protection legislation.

What should Internal Audit teams think about?

Third line teams should be aware of the current ICO focus as part of the Data agenda, and the potential impact of data on current activities.

- Advertising technologies - given the renewed focus on cookie compliance, internal audit teams should assure that Risk and Compliance teams have effectively reviewed existing cookie arrangements, and be aware of the requirement to notify individuals of the existence of cookies, clearly explaining the purpose of each cookie, and finally obtaining an individual's explicit consent to store a cookie on their device. Essentially, the firm should ensure that the option to reject cookies is clearly highlighted.
- Artificial Intelligence – for AI technologies already in use within the sector, firms would do well to keep an eye on the ICO's consultation series on generative AI, with the first chapters published focusing on the lawful bases used for web scraping to train GenAI models, and how purpose limitation should be applied at different stages of the AI lifecycle. From a governance perspective, internal audit teams should ensure that AI technologies are not developed in siloes, but instead developed, implemented and monitored with input from data protection compliance teams from the outset (demonstrating a 'privacy by design' approach), as well as other relevant stakeholders from across the organisation, including risk, legal, IT security, data scientists and senior management.

Case Study - Recent ICO enforcement action on an FS firm

In January 2024, the ICO issued a £50,000 financial penalty to an FS firm for being in breach of regulations 22 and 23 of the Privacy & Electronic Communications Regulation (PECR) for sending over 30,000 direct marketing text messages without valid consent. The enforcement notice highlighted that individuals were not given the opportunity to 'opt-out' of receiving further messages.

Financial services firms should be aware that the requirements for processing on the basis of consent are high, under the UK data protection legislation and the onus is on the data controller to evidence the collection of consent from each individual. Some considerations for an organisation relying on consent as a legal basis include:

- Ensuring any consent collected constitutes an unambiguous indication of an individual's wishes, so 'opt-in' not 'opt-out' (passive consent is not permitted);
- Consents are not 'bundled together' or captured for multiple data processing activities, but must be clearly distinguishable;
- Consents are written in clear plain language, so that the individual can clearly understand what they are consenting to;
- Ensuring that for direct marketing, the option for individuals to 'opt-out' of future marketing emails should be clearly highlighted on each communication; and
- Organisations should also maintain a record of consents, including the time/date evidence was obtained in the event of any challenge.

What should Internal Audit teams think about?

The ICO continues to be active in issuing enforcement action, including financial penalties non-compliance with nuisance marketing texts and/or emails across different sectors. To reduce the risk of individuals making complaints directly to the ICO and avoid some of the pitfalls highlighted in the example above, internal audit teams should review that consent arrangements are aligned to the requirements of UK data protection legislation and PECR, and refer to the ICO guidance for Direct Marketing and Regulatory Communications, specifically for regulated sectors.

It is also worth noting that the FCA's Consumer Duty (which came into force for existing products in July 2023) will come fully into force in July 2024 for closed products or services. Under the duty, firms should actively communicate with customers about products and services. In order to understand consumers, however, consideration should be given to whether Consumer Duty driven communications with customers potentially cross over into direct marketing. If a regulatory communication constitutes direct marketing, the firm must give individuals the right to object to being sent such direct marketing. The ICO has provided guidance on direct marketing and regulatory obligations.

For further information regarding how to navigate the changes, or if you have any questions, please reach out to Christopher Beveridge, Managing Director of Privacy and Data Protection, or Louise Sadler, Senior Manager, Privacy and Data Protection.

04

ESG Update

ADAM SOILLEUX
Director

adam.soilleux@bdo.co.uk

GLORIA PEREZ TORRES
Associate Director

gloria.pereztorres@bdo.co.uk

From Net Zero strategies to Transition Plans: How can Internal Audit support evolving expectations?

A transition plan is an integral component to a firm's overall strategy in that it sets out the plan to contribute to and prepare for a transition towards a lower GHG-emissions economy. Transition plans have the core purpose of explaining how an organisation will meet climate targets, manage climate-related risks, and contribute to the economy-wide climate transition.

To help financial institutions and other organisations to produce the highest standard for best practice climate transition plans, the Transition Plan Taskforce (TPT) was launched by HM Treasury in April 2022. Importantly for the financial services sector, the TPT has developed a Disclosure Framework with the intention of providing organisations with guidance on how to develop credible, robust climate transition plans as part of their annual reporting on their forward business strategy. This is because the credibility and integrity of transition finance has been a focal point for stakeholders.

The production of the Disclosure Framework was part of the TPT's wider role within HM Treasury. The initiative was announced at COP26, in November 2021, began operations in April 2022 and was the first area opened for consultation in November 2022. In November 2023, consultation began on Sector Deep Dives, which are scheduled to be published in Spring 2024. Additionally, in January 2024, the TPT began contributing to the Transition Finance Market Review, with an accompanying Forward Pathway on transition plans intended to be published in Summer 2024. Most financial services firms have already developed Net Zero Plans and the PTP framework will support them in further developing these plans into more comprehensive decarbonisation plans to transition into lower GHG emissions.

Key considerations for transition plans

Generating a credible, effective, comprehensive, and compliant climate transition plan is one of the greatest challenges facing firms in financial services. Achieving these decarbonisation targets requires expert knowledge of new legislation and climate-related guidance initiatives in the context of how they apply to a firm's specific business sub-sector e.g., banking, asset managers, etc. Climate transition plans must cover a wide range of a business' impact on, and engagement with, society.

The TPT recommends any transition plans are based around the following four pillars:

- Implementation Strategy: The implementation strategy is expected to cover typical business operations, a firm's products and services, policies and conditions, and financial planning.
- Engagement Strategy: Firms are expected to disclose their engagement financed emissions and, with supply and value chains, how they intend to engage with industry, and how they intend to engage with bodies from the government, public sector, and wider civil society.
- Metrics & Targets: Disclosure must include measurable progress on climate-related issues, including financial metrics and targets, GHG metrics and targets, and carbon credits (when applicable).
- Governance: Effective governance is central to suitable accountability for a climate transition plan. Board oversight, the role of management, company culture, and incentive / renumeration packages are all expected areas of disclosure.

To be successful in embedding each of the above in their climate transition plans, firms will require well-designed internal controls to ensure that their new processes for producing climate-related disclosures operate as intended. Climate transition plans cover the length and breadth of an organisation's operations, from regular business activity, financed emissions and investments, metrics and targets, and company culture.

What should Internal Audit teams think about?

Effective utilisation of an internal audit function will make a significant difference for firms, whether or not they currently have a transition plan. For firms who have already designed a Net Zero or transition plan, internal audit can provide strenuous testing for both the design and operational effectiveness of their plan. Such testing provides firms with recommendations for improvement, alongside the confidence that they can embed their ESG strategy and achieve their ESG targets. This will contribute to increasing transparency and credibility of the plans.

Firms who are yet to design and implement a transition plan would also benefit from the input of an internal audit function. Taking TCFD disclosures as a starting point, internal auditors can review the current framework of metrics and targets and provide advice and expertise on what is a new and specialised field to ensure that firms are aware of what is expected from them in the coming years and the steps they will need to take to ensure regulatory compliance. Currently, markets can mitigate their own risks regarding climate transition plans and climate-related disclosures. Internal audit can help firms take advantage of this opportunity.

How can Internal Audit support evolving expectations?

Internal auditors can also use transition planning guidance and recommendations to assist firms in shaping their own ESG strategies. The four pillars of the climate transition plans stipulated by the TPT could be effectively utilised by internal audit when assisting firms in the early stages of deciding on ESG targets and strategies.

Internal audit teams should take a more holistic approach, whereby ESG challenges are viewed as part of a wider issue to be tackled, as opposed to a collection of separate problems to be addressed.

Current trends clearly indicate one direction of momentum regarding climate-related disclosures. Firms would do well to heed them and start preparing for mandatory disclosure of climate transition plans as soon as practicable.

Regulatory updates are expected in the UK sooner rather than later. The FCA indicated in August 2023 of its intention to consult on transition plan disclosures by listed companies in line with the TPT Disclosure Framework, alongside its consultation on implementing UK-endorsed ISSB Standards. The FCA's new requirements are expected to be enforced for accounting periods from January 2025, with the first reporting beginning from 2026.

05

Economic Crime Update

VLADIMIR IVANOV
Senior Manager

vladimir.ivanov@bdo.co.uk

Economic Crime Update

FCA Business Plan 2024/25

On 19 March 2024, the FCA published its Annual Business Plan for 2024/25 setting out its planned programme of work for the coming year.

The Business Plan sets out that the FCA will continue to deliver on its 13 public commitments which are focussed on:

- reducing and preventing financial crime
- putting consumers' needs first
- strengthening the UK's position in global wholesale markets.

In respect of reducing and preventing financial crime, the Business Plan notes that the FCA will continue to take a data-led approach to identify potential harm for supervisory and/or enforcement action. The Plan further splits the FCA's desired outcomes and key activities for the period. Some of the core points highlighted are as follows:

Outcomes the FCA wants to achieve

- slowing the growth in investment fraud victims and losses
- slowing the growth in Authorised Push Payment (APP) fraud cases and losses
- reducing financial crime by lowering the incidence of money laundering through supervised firms

Key activities the FCA will start in 2024/25

- Increasing investment in systems to use intelligence and data more effectively within its Financial Crime work, so it can target higher risk firms and activities.

Key activities the FCA will continue in 2024/25

- Using its powers to disrupt, pursue and sanction those committing and enabling financial crime.
- Improving its capabilities to identify and request platforms remove unauthorised financial promotions, associated websites and social media accounts.
- Raising awareness of fraud through its consumer campaign.
- Focussing on proactive assessments of Anti-Money Laundering ("AML") systems and controls for those firms deemed higher risk.
- Using data to target the firms that are more susceptible to receiving the proceeds of fraud and ensure they do more to stop the flow of illegitimate funds.
- Strengthening its supervision of firms' sanctions systems and controls.

The Business Plan also notes that the FCA will seek to significantly increase its capability to tackle Market Abuse. Some of key work which the FCA will seek to carry out includes:

- Increasing its ability to detect and pursue cross-asset class market abuse and developing improved market monitoring and intervention in Fixed Income and Commodities.
- Assisting in delivering a proportionate Market Abuse regime for Crypto Assets.
- Publishing the results of its peer review of Market Abuse systems and controls in providers of Direct Market Access.

What should Internal Audit teams think about?

Whilst the Business Plan is relatively high level, firms should pay close attention to the FCA's areas of focus for the year ahead.

Unsurprisingly, fraud prevention is a top priority for the Regulator. In the midst of the 'Failure to Prevent Fraud' offence (implemented through the Economic Crime and Corporate Transparency Act 2023) and the continued Government focus on reducing fraud within the UK, it would not be a stretch for the FCA to begin proactively assessing firms' fraud prevention systems and controls. Internal audit teams should, therefore, ensure that sufficient resources are devoted to reviewing fraud risk management frameworks.

AML and sanctions remain as high priority areas for the FCA. Firms should, therefore, continue to ensure that their frameworks are benchmarked against regulatory requirements and industry best practices and that their systems and controls are subject to frequent oversight and testing.

FCA 'Dear CEO' letter to Annex 1 Firms

On 5 March 2024, the FCA published a 'Dear CEO' Letter setting out its findings from recent assessments of a number of Annex 1 firms in order to evaluate how they are complying with the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) (as amended).

There are approximately 1,000 Annex 1 registered firms, which are not authorised or subject to wider FCA regulation. These include some lenders, safe custody providers, money brokers and financial leasing companies, which undertake specified activities which requires them to be registered and supervised by the FCA for compliance with the MLRs.

Economic Crime Update

The letter outlines some of the weaknesses which the FCA commonly identified across its assessment population of Annex 1 firms, namely:

Business model

- Discrepancies between the activities that firms have told the FCA they would undertake when they registered, and the activities firms told the FCA they undertake when asked during the assessment.
- Firms' Financial Crime policies, procedures, and controls not keeping pace with the size and complexity of the business, resulting in an inadequate Financial Crime framework.

Risk Management

- Completely absent or poor-quality Business-Wide Risk Assessments ("BWRA")
- Customer Risk Assessments ("CRA") not being sufficiently tailored to customers' characteristics.

Due Diligence, Ongoing Monitoring, and Policies and Procedures

- Policies and procedures lacking sufficient detail over: the level of Due Diligence to be applied; if/how ongoing monitoring measures are applied; and the investigation and recording of Suspicious Activity Reports ("SARs")
- Policies and procedures being vague on staff responsibilities.
- Policies and procedures not being kept up to date.

Governance, Management Information and Training

- Firms' Financial Crime Prevention teams not being adequately resourced to carry out their functions effectively and/or there being insufficient senior management oversight.
- Financial Crime training not including role-specific training for employees and/or failing to cover crucial topics.
- Financial Crime not being a standing agenda item at senior management meetings, resulting in the absence of a clear audit trail to support Financial Crime decision making.

What should Internal Audit teams think about?

Whilst the 'Dear CEO' Letter is not principally targeted at the majority of the sector, regulated firms should consider the top-line messages regarding identified vulnerabilities. Thematic publications from the FCA provides helpful intelligence regarding the expectations of the Regulator in respect of firms' financial crime frameworks.

Internal audit teams within all firms subject to the MLRs should, at a minimum, consider the letter as part of financial crime risk assessments and ensure second line teams are reviewing its implications, assessing financial crime frameworks for the common failings highlighted, and consider review of the audit plan to ensure upcoming assurance activities are appropriately tracking risks.

06

Digital Update

JASON GOTTSCHALK
Digital Partner

jason.gottschalk@bdo.co.uk

RACHEL FALLON
Digital Senior Manager

rachel.fallon@bdo.co.uk

Digital Operational Resilience Act (DORA)

The European Union Council adopted the Digital Operational Resilience Act (DORA) regulation to ensure that digital infrastructure, including the systems and networks that underpin critical services in the financial sector, is secure and resilient against potential threats. While cyberattacks cannot be avoided, financial stability in Europe can still be achieved if organisations mitigate the impact of cyber threats on information and communication technologies (ICT). The objective of DORA is to improve the cybersecurity and operational resilience of all regulated European financial institutions and of critical, third-party ICT service providers.

To whom does it apply?

DORA applies to a wide range of organisations, including regulated financial services firms and ICT third-party service providers, such as cloud computing services, software, data analytics services and data centres.

DORA puts the relationship between the financial institutions and their technology suppliers in a new light to jointly address the regulatory requirements. Financial entities and ICT third-party service providers should increase their collaboration to address the requirements of this new regulation.

What are the DORA Requirements?

Overall, responsibility for this implementation of DORA and other governance obligations imposed by DORA, will rest on the firm's management, which will be responsible for reviewing, approving, implementing and updating the risk management framework. Management will be required to have full awareness and understanding of the financial institution's ICT usage, services and risk profile. Companies may want to assess how reporting lines from their ICT department to senior management operate daily. The financial institutions that are subject to DORA must appoint a senior executive responsible for digital operational resilience and report incidents to the appropriate authorities.

When will DORA be implemented?

In December 2022, DORA was announced in the journal of the EU. Following, the general regulation, technical standards (RTS) were published in January 2024. DORA will be implemented on 17 January 2025.

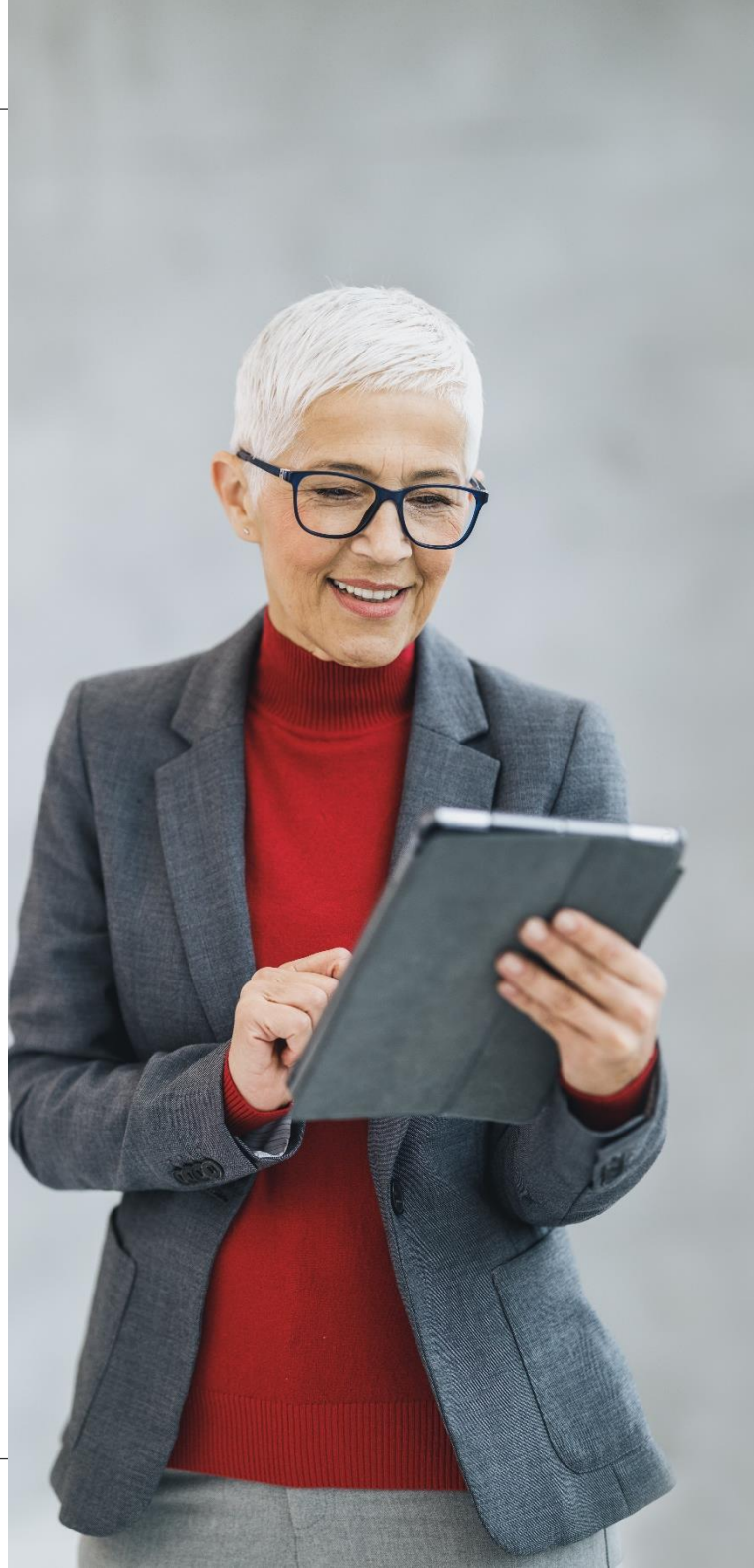
What should Internal Audit teams think about?

Achieving compliance with the onerous DORA obligations within the stipulated timeframe will be challenging and time-consuming. While DORA allows a transition period until 17 January 2025, internal audit teams should check that appropriate preparations have been put in place by the firm's second line.

Given the substantial programme of work to deliver compliance by January 2025, internal audit teams should develop a phased approach, whereby assurance providers coordinate their activities to support compliance over the transition period. This should include periodic reporting to Board and senior management on the assurance activities supporting compliance change management.

Internal audit teams should also consider cosource partners to provide support on the function's key review activities during the transition period, such as:

- Performing a DORA gap analysis and assess the firm's current cyber maturity and resilience level.
- Defining a prioritised roadmap that includes DORA requirements and associated compliance with other applicable legislation and regulations.
- Supporting project management and/or hands-on execution of the security roadmap, e.g. putting in place key policies and procedures, performing resilience testing, managing the penetration testing and implementation of subsequent recommendations, performing third party/vendor risk assessments, etc.



FOR MORE INFORMATION:

Richard Weighell

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

www.bdo.co.uk

XXXXXXX