INTERNAL AUDIT SUPPORT

BANKING & BUILDING SOCIETIES

November 2023

IDEAS | PEOPLE | TRUST

BDO

BDO FS INTERNAL AUDIT CONTACT POINTS

We recently launched a new survey to help gather some helpful benchmarking data across our readership.

A link to our short 5-question survey can be found on here: IA Benchmarking Survey

Following feedback from our readership, we have extended the deadline for responses to ensure we've captured a broad set of perspectives regarding 2024 plans. We will publish a summary of the responses and some analysis on what the data tells us in December's edition.

****

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

DATA PROTECTION UPDATE

SUBJECT ACCESS REQUESTS

CHRISTOPHER BEVERIDGE
Managing Director of Privacy and Data Protection

DATA PROTECTION UPDATE

Subject Access Requests

Following a number of recent high-profile subject access requests over the summer, firms within the financial services sector are reviewing their processes to ensure that they do not make the headlines for non-compliance in this area.

WHAT IS A SUBJECT ACCESS REQUEST?

The UK General Data Protection Regulation (UK GDPR), which is enshrined in domestic legislation as the Data Protection Act (2018), affords individuals several rights in relation to their personal data, including the right to access, which is commonly known as a 'subject access request'. Individuals have the right to access and receive a copy of their personal data and other supplementary information, and firms are required to provide this information, although it should be noted that such a request can also be refused if it is deemed to be manifestly unfounded or excessive.

Individuals can make a subject access request verbally or in writing, including via social media.

Firms are required to process subject access requests within one calendar month, which can be extended by a further two months if the request is overly complex or onerous, and in the most circumstances, firms cannot charge a fee to deal with the request.

Whilst the intention of the right of access is to increase transparency, and to enable individuals to determine whether their personal data is being used in accordance with data protection laws, in practice, subject access requests are often used by ex-employees or disgruntled customers who are looking for specific information, or want to cause disruption (this especially in the case of a long-standing employee, where the number of documents containing personal data can run into the thousands).

Either way, in view of the enforcement powers of the Information Commissioner's Office ('ICO') (and associated reputational damage), financial services firms should be fully cognisant of the risks associated with getting this wrong and Internal Audit team should appropriately plan for data protection reviews.

DATA PROTECTION UPDATE
Subject Access Requests

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

People

- Are employees aware of the process in the event of a data subject rights request, where strict time limits apply? Employee awareness is a key control to ensure that prescribed time limits are adhered to. Organisations should, therefore, be considering whether employees receive sufficient training to identify, (and for specific teams) manage subject access requests.
- Have sufficient resources been allocated to managing subject access requests in line with prescribed timescales? If an organisation has seen an increase in the number of subject access requests received, have sufficient resources been allocated to meet the demand in line with the regulatory timescales?

Process

- Have processes for managing subject access requests been defined? Subject access requests can be tricky and lengthy to navigate, especially when it comes to verifying the identity of the requestor, applying an extension, managing exceptions or instances in which a request can be refused, finding and retrieving the data, redacting/removing personal data pertaining to other individuals and providing the data to the requestor within the prescribed timeline. All these considerations highlight the importance of formally documenting processes for managing subject access requests.
- Does management have oversight of compliance with key timescales? Depending on the volume of subject access requests received, exceeding the one calendar month deadline for managing a request, or regularly applying an extension for basic requests, can be indicative of wider issues, such as a lack of dedicated resource to manage subject access requests.

Technology

- Are processes for extracting and redacting personal data automated or manual? Depending on the volume of subject access requests an organisation receives, an overreliance on manual processes for extracting and redacting personal data can lead to inefficiencies and increase the risk that prescribed deadlines could be missed.

DATA PROTECTION UPDATE

Subject Access Requests

ICO REGULATORY FOCUS

As highlighted above, the ICO has a range of enforcement powers at its disposal, including monetary penalties, enforcement notices, undertakings, reprimands and, in some cases, individual prosecutions. However, if the press coverage of recent high-profile cases is anything to go by, internal audit teams should be mindful of any associated reputational damage arising from enforcement action taken, which is published via the ICO website on an ongoing basis.

Further to this, it's worth noting that an organisation has recently received a reprimand from the ICO, for failing to process 35% of subject access requests within the statutory deadlines of one and three months, so the ICO is focusing on this.

Following a number of headlines over the summer, the topic of subject access requests remains a key area of focus within the sector, and our specialist team is available to provide support.

For further information, 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.

02

BEHAVIOURS & CULTURE

WHY IT MATTERS – PART 1

ALISON MACKEY
Associate Director

BEHAVIOURS AND CULTURE

When we look at recent and past examples of firms collapsing or scandals in the sector, one thing connects them all – behaviours and culture.

The UBS 'rogue' trader Kweku Adoboli was jailed in 2012 for unauthorised trading which had led to a loss of USD2.3bn for the organisation. UBS moved quickly to distance itself from the scandal, leading to Adoboli being labelled as a 'bad apple' and a symbol of 'banker's greed' at a time when public trust in the banking sector was at rock bottom. Adoboli's case is an example of the need to deeply explore the broader culture of firms and the environment which allows, and often encourages, undesirable behaviour. Former employees have since talked about UBS' focus at that time as being on 'individual advancement over team efforts' and 'every man for himself'.

Before the financial crisis in 2008, it was hard to find anyone really talking about 'corporate culture' in financial services – let alone trying to understand it. Since then, regulators and leaders in the industry recognise that the culture of an organisation was as key a factor to the crisis as risk management. But you could argue that behaviours and culture remain a blind spot for so many organisations. This also extends beyond financial services into other sectors, healthcare being one.

The recent cases of Silicon Valley Bank (SVB) and Credit Suisse bring this into stark focus. Toxic culture and poor risk management were the root causes to both firms failing.

- Both organisations had been undergoing significant strategic transformation with a focus on short-term growth which created new and increased risks.
- At SVB, there was a lack of internal challenge to what was clearly a risky strategy.
- Leaders at SVB were not open to challenge from the regulator. There was also no CRO in-role for around one year.
- At Credit Suisse, many leaders left of their own accord when the new strategy was announced, to which the Chief Executive responded by giving decision making power to those in the executive management committee who supported his strategy.

SVB failed very quickly. Credit Suisse took longer, with a combination of trading losses and reputational damage taking its toll over a few years until the bank collapsed. What is clear is that factors such as pressure from the top on growth and profit, lack of challenge and accountability and de-prioritisation of risk did such seismic damage, there was no chance of recovery.

The regulatory expectations are set around the need to determine, understand, measure, monitor and report on culture and behaviours. However, so many organisations continue to struggle with quantifying what they see as intangible risks.

BEHAVIOURS AND CULTURE

Internal Audit plays a crucial role in identifying risks and issues in relation to behaviours and culture and helping Board and Executive teams understand why this is a business-critical issue. The CIIA's 'Internal Audit Financial Services Code' sets out expectations of IA's role in assessing culture and its indicators:

"Internal audit should include within its scope the risk and control culture of the organisation. This should include assessing whether the processes, actions, 'tone at the top' and observed behaviours across the organisation are in line with the espoused values, ethics, risk appetite and policies of the organisation…".

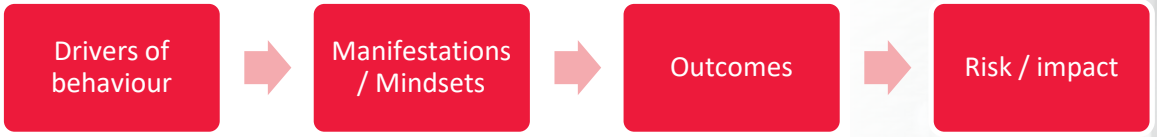
However, IA functions have had varied success with fulfilling this mandate.

Auditing culture is complex….

- There is no one-size-fits-all model to apply.
- You cannot diagnose a culture in just one audit.
- Changes to behaviour and culture take time and cannot be addressed by just implementing a suite of controls!

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

To understand where there are potential risks to the organisation, we must understand behaviours – the culture that we can see. The following model is a simple way of thinking about behaviours and culture from a risk perspective where behavioural drivers are the root cause, ultimately resulting in a risk:



However, first you need to understand more about the organisation's culture.

Certain firms will be more advanced in their thinking about behaviours and culture, therefore building our understanding of where your firm sits on that scale is an important starting point.

BEHAVIOURS AND CULTURE

Consider asking some key questions:

How do you describe your organisation's culture?

- You are looking for a clear and compelling purpose, linked to values and expected behaviours.
- Post the question to different groups of stakeholders, i.e., the Audit Committee, Board, C-suite and any junior managers. Expend effort to include management and teams that have relatively less interaction with the IA team. It is interesting to note where the 'culture' is interpreted in different ways as this may provide insights to potential areas for focus.

How is that culture communicated to your people? How do you get feedback?

- Think about the ways in which the firm's culture is shared – is it just a published statement on the corporate website, or is it brought to life in other ways?
- The openness to feedback and for leaders to demonstrate a 'listening' culture is critical. There is a tendency to rely on limited data when gauging the workforce's buy-in.

What do you do to reward and recognise your people?

- Remuneration is one aspect – how do remuneration practices incentivise and disincentivise behaviour?
- Look to understand how mobility across the firm is managed and encouraged. Are certain teams in the firm impenetrable silos, limiting movement in or out?
- How do leaders ensure there is psychological safety for people, i.e., people feel that the team is safe for interpersonal risk taking, feedback and opinions can be shared without the fear of repercussions.

By asking questions such as these as part of your ongoing engagement with auditees and/or part of certain audits, you can start to build a picture as to where a deeper dive into specific areas may be of value. You may already have a clear idea of potential behavioural/cultural issues within the firm and want to perform specific audit work to provide assurance in this area.

Areas to potentially focus on include:

Risk Culture: *transparency, accountability, prioritisation*

Leadership: *style, decision making, communication*

Dynamics between teams/business areas

03

CONSUMER DUTY UPDATE

AN UPDATE FOR INTERNAL AUDIT TEAMS

ALISON BARKER
Special Adviser

CONSUMER DUTY UPDATE

The FCA's Consumer Duty implementation date on 31 July 2023 (for existing products and services) has passed and we are now into a period of embedding and review by FCA. This article sets out some of the hot topics, risk areas and questions the regulator is posing, plus highlights the next milestones for implementation and review.

Just to recap, the FCA's Consumer Duty is extensive and wide-ranging consumer regulation that seeks to improve outcomes for retail consumers and SMEs. We have previously summarised the new regulatory requirements and links to previous articles published on our website can be found here.

As set out in the FCA's Business Plan, published in April, it is now focusing on the successful embedding of the Consumer Duty into firms' systems and controls. The regulator has a budget of £5m and we are starting to see some of the outcomes from the FCA's supervisory work:

- supervisory teams are carrying out a range of thematic and firm-specific reviews;
- we are seeing some very detailed information requests seeking analysis at a product or customer journey level
- FCA teams are requesting detail regarding gaps or harm identified and action plans in place to address these areas.

It is a learning process and there are no definitive responses for all cases. Over the next 12 months, we expect to see a greater level of consensus about what 'Good' looks like.

HOT TOPICS FROM OUR MARKET EXPERIENCE

Price and value

There has been specific focus across sectors on fees and charges and fair value for consumers. As a reminder, one of the four consumer outcomes is headed Price and Value.

We want all consumers to receive fair value. Value is about more than just price, and we want firms to assess their products and services in the round to ensure there is a reasonable relationship between the price paid for a product or service and the overall benefit a consumer receives from it.(FCA Policy Statement 22/9, 7.1.)

Given the cost-of-living pressures for consumers and small businesses, FCA is focused on fair value, and we are seeing plenty of press coverage on topics, such as interest rates and commission charges to leaseholders. There should be a reasonable relationship between price, value and work done. Assessments of fair value need to be detailed and at a customer cohort level to identify customer groups where fees and charges may not show a reasonable link to price or value. It is an analytical process and a judgement on what is reasonable. The FCA expects action to reduce fees, change charging structures or disclosures where needed. The hardest discussions within a firm's senior management will be about reducing fees and charges.

CONSUMER DUTY UPDATE

Consumer Journeys and foreseeable harm

We are seeing requests for information about the granularity of consumer journey mapping, harm identified, and actions being taken. As a reminder, the consumer understanding and support outcomes, require firms to take a close look at processes that act as a barrier to consumers achieving their financial goals. A thorough evidenced rationale for customer journey mapping, issue identification and action plans and action tracking should be in place.

Added to this is the ability for firms to think about foreseeable harm. The Consumer Duty rules expect firms to identify what is reasonably foreseeable and act accordingly. For example, the rise in interest rates should have prompted a new risk assessment to identify issues ranging from operational capacity to deal with consumer calls to how interest rises are passed onto consumers.

Vulnerable Customers

Areas of focus also include identification and treatment of vulnerable consumers through customer journeys. Vulnerability is sometimes a difficult concept to operationalise for firms. Identification and assessment processes may not be well advanced, and we have seen FCA challenging the quality of MI in place to assess outcomes for vulnerable consumers.

Root Cause Analysis

There should be a range of metrics in place to measure outcomes. What will be important is the root cause analysis of identified issues and actions to address. This might be at a process, control or competency level, or a more strategic understanding of how a business model is operating. Our observation is that the FCA is challenging the quality of root cause analysis and extent to which strategic as well as process issues are identified.

The Annual Review

The responsibility of Boards this year will be to review and assess how they are meeting the Consumer Duty. The FCA's Final Guidance (FG 22/5) 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 is specifically asking about the role of second and third lines in the review and reporting process and challenge to first line or support to the Board in its review role. Boards should be looking for assurance from second and third lines that metrics, reports and actions have sufficient breadth and depth of coverage and effective root cause analysis.

We have published a specific article about the annual review process here.

It would be reasonable to assume that any annual reports to, and reviews by, the Board will be subject to FCA scrutiny and, therefore, a good quality evidence-based discussion is important to demonstrate rationales for decisions, actions taken and progress towards embedded consumer culture.

Closed Books - 2024

As a postscript, we must not forget that for closed products, those no longer sold or renewed, the deadline for implementation of the Consumer Duty is 31 July 2024. The requirements are slightly different. Plans should be in place and well advanced. Some actions could be complex and should be highlighted as a risk area. For example, some potential issue areas could be missing product terms and conditions, exit charges, reduced levels of customer service and support in comparison to existing products and services on sale. Internal Audit teams should have specific focus on the risks for closed book Consumer Duty implementation projects and the costs of any potential actions.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

- This is still an evolving regulatory initiative with emergent themes and Hot Topics. The industry, as much as the regulator, is learning as the regulatory process unfolds;
- Second and third lines should be providing meaningful and well documented challenge to support embedding of the new Duty and ensure that the annual review process is taking place;
- 2024 sees the first Annual review by the Board and deadline for implementation for closed book. Internal audit teams should update the annual audit plan to incorporate appropriate assurance activity at key milestones for this process.

04

ECONOMIC CRIME UPDATE

CLARINDA GRUNDY
Associate Director

ECONOMIC CRIME UPDATE

FCA SHARES REVIEW OUTCOMES RELATING TO DETECTING AND PREVENTING MONEY MULES

On 19 October 2023, the FCA published key findings from its review of payment account providers' systems and controls against money mule activity. The aim of the publication was to share good practices and areas for improvement about how firms manage the risks of money mule accounts in a proportionate manner. The FCA explicitly notes that MLROs in Banks and Building Societies should take heed of this publication.

In the publication, the FCA reminded firms that fraud currently accounts for 40% of all crime and that the ease with which fraudsters cash out the proceeds through mule accounts continues to be a problem.

The FCA clarifies that its review identified three key areas of good practice:

- **Systems and controls** – amongst other things, the FCA commends the proactive use of innovation and technology to deploy solutions including facial recognition systems, device profiling and geolocation;
- **Use of intelligence, industry engagement and data sharing** – the FCA notes that collaborative tools such as data sharing pilots have proven to be beneficial; and
- **Training** – the FCA notes that dedicated staff training initiatives are having a positive impact.

However, the FCA identifies that more work is needed in areas such as:

- Governance, management information (MI);
- Risk assessment;
- Onboarding;
- Transaction monitoring;
- External reporting;
- Resourcing; and
- External communication and awareness.

The FCA expects firms to establish and maintain proportionate systems and controls to manage money mule related risks and warns that it is at liberty to employ a range of regulatory tools in instances where failures are identified.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

Internal Audit teams should be alive to evolving fraud and money laundering threats and the role that mules may play in enabling illicit activity to take place. Some key considerations for audit planning include:

- Identifying and documenting existing and emerging mule typologies both with respect to money laundering and fraud
- Building these into onboarding and ongoing monitoring processes by undertaking appropriate and proportionate checks at onboarding to identify indicators and red flags of mule activity and deploying robust ongoing relationship monitoring strategies to detect common mule behaviours for inbound as well as outbound transactions
- Implementing timely external reporting protocols, supported by controls such as Service Level Agreements, to support intelligence sharing and, ultimately, the closing down of mule networks; and
- Enhancing communication strategies and awareness initiatives to keep customers abreast of the latest threats and challenges, especially against the backdrop of the ongoing cost of living crisis and how this impacts personal vulnerability.

ECONOMIC CRIME UPDATE

SANCTIONS COURT CASE PROVIDES INTERESTING OUTCOMES

On 6 October, the UK Court of Appeal ('CoA') issued its judgment in a case brought by Boris Mints & others v PJSC National Bank Trust & PJSC Bank Okritie. The case centred around the extent to which a sanctioned party (designated person) could be considered to 'control' an entity and thus the sanctions applicable to the designated person also extend to the entity. In this instance, the case related to sanctions against Russian President, Vladimir Putin.

The outcome was that a designated person would be considered to 'control' an entity where the entity is not a personal asset of the designated person, but the designated person is able to exert influence over it by virtue of the political office that the designated person holds. Further, the judge stated that "in a very real sense,…..Mr Putin could be deemed to control everything in Russia".

The case brought significant interest given the grey areas in interpretation of the ownership and control clauses cited in applicable sanctions regulation.

On 16 October, the UK Foreign, Commonwealth & Development Office ('FCDO') issued a statement which noted that the UK Government is "carefully considering the impact" of the outcomes of the case. Importantly, it clarified that *"There is no presumption on the part of the Government that a private entity based in or incorporated in Russia or any jurisdiction in which a public official is designated is in itself sufficient evidence to demonstrate that the relevant official exercises control over that entity"* but is committed to exploring options to further enhance clarity in this area going forwards.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

This further exemplifies continued need for focus on the sanctions compliance agenda, discussed in our October update. In addition to the FCA-driven focus areas, internal audit teams should consider:

- Gaining familiarity with the Boris Mints & others v PJSC National Bank Trust & PJSC Bank Okritie case and analyse how similar situations may occur in their own firm;
- Horizon scan and monitor for UK Government and/or OFSI updates or guidance because of the outcomes of this case; and
- In the interim, revisit internal definitions and guidance relating to beneficial ownership and control to ensure that their frameworks provide sufficient clarity and guidance relating to the instances in which entities may be subject to sanctions by virtue of their direct or indirect ownership or control by a designated person, and that staff are aware of items which may need escalation as well as instances which are deemed outside of risk appetite.

FOR MORE INFORMATION:

RICHARD WEIGHELL
Partner

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

www.bdo.co.uk

42020160