INTERNAL AUDIT SUPPORT

BANKING & BUILDING SOCIETIES

October 2023

IDEAS | PEOPLE | TRUST

BDO

BDO FS INTERNAL AUDIT CONTACT POINTS

Following on from our Planning edition, we have now 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 page 7 and, provided we have a meaningful set of responses, we hope to publish a summary of the responses and some analysis on what the data tells us in November'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

MEET THE TEAM

MICHAEL HADDON
Principal, Financial Services Advisory

MEET THE TEAM

Each month, we shed more light on our FS Internal Audit practitioners so that we can get to know the person behind the practice in 10 questions. This month, we get properly introduced to Michael Haddon.

1. What has been your career leading into BDO?

I've been on the road a fair bit. Prior to joining BDO in 2013, I spent 13 years with KPMG and PwC in Bangkok, 10 years with KPMG in London and 5 years with a medium sized accounting firm based in Covent Garden (where I trained and qualified as an ACA).

Most of my time has been spent providing external and internal audit assurance, transaction services and risk management advisory across financial services.

My role in Thailand needed me to dive into a lot of situations which were a little out of my comfort zone but the payback was worth it. The range of experience gained really helped when I returned to the UK and joined BDO. I was also part PwC's Global Account Team for a global blue-chip firm, a team that delivered USD50 million of advisory work in a good year and some of that came from our team in Thailand.

I also spent a few years helping develop PwC's advisory practice in Cambodia where one of my favourite assignments was at the Tiger Beer Brewery just outside Phnom Penh!

2. Describe your role in the FS Internal Audit team?

I support the partners and colleagues to deliver cosourced and outsourced internal audit services, primarily to the banking sector. On our larger accounts, this means spending a lot of time at clients, aiming to be perceived as 'part of the team' and acting as a sounding board and a source of support beyond our core internal audit work. That part is very rewarding.

As a senior member of the team, I also help to produce and deliver thought leadership materials and client facing events, such as roundtables.

These are great opportunities for really testing just how much you really know and working out how best to get some good content across to the audience.

I also play a role helping to build and develop our internal team and enhance the way we do things. Onwards and upwards!

3. What's the most interesting thing you're working on right now?

I'm helping the Group Head of Internal Audit at one of our main cosourced clients to transition to a bigger in-house function. This involves helping identify opportunities to enhance the function's overall operating effectiveness, in line with the expectations for a Category 2 regulated bank. The brief includes helping implement more short-term tactical solutions while building out a target operating model and a more strategic, forward-looking plan. This support also involves meeting with several stakeholders to hear their views on internal audit and this is always interesting.

4. Best thing about being part of the Internal Audit Team?

The variety of the work and client cultures, together with the diversity within our team makes for an interesting and fun time.

5. What drives you to do what you do?

I really enjoy trying to understand how and why people and organisations do the things they do – I'm quite analytical. This helps me better understand how I might want to approach things at many different levels, always anchored around seeking to 'do the right thing'. To achieve this, it's important for me to see the big picture so I can put matters into context and so offer an informed view or opinion.

6. What's something that has surprised you about your Internal Audit career path?

It really provides fantastic breadth and depth of experience and this helps me develop rounded views, resulting in far more meaningful conversations with clients and colleagues.

7. What's the best piece of professional advice you've ever received?

Write as you speak!

8. How do you see internal audit changing over the next few years?

Stakeholders are needing increased levels of real-time and/or data driven assurance and so ensuring we can deliver this through technology will be a challenge, but one we must embrace if we wish to remain relevant and competitive.

9. What is your favourite thing to do when you're not working?

I'm an active person (and a little bit competitive) so a lot of my free time is taken up with sports – football, tennis, golf, walking in the hills, as well heading to an 'older persons' gym.

I also like art – appreciating a great work is satisfying but equally, I love to hear what the artist was doing/aiming to reflect in the painting. Makes it much more interesting.

10. If you were stranded on a desert island, what three items would you want to have with you?

If the sun was always going to shine, I'd probably stay there so a fishing rod, the complete works of Shakespeare and a top end bottle of wine (that will never get opened).

02

INTERNAL AUDIT BENCHMARKING

RICHARD WEIGHELL
Partner

INTERNAL AUDIT BENCHMARKING

A new IA benchmarking survey

In our previous edition, we explored the key planning considerations for 2024 plans.

The scale and complexity of the regulatory change, macro-economic factors, emerging business risks and technological developments that need to be incorporated into risk-based audit plans is immense. Heads of Internal Audit have an incredibly complex task of managing an ever-larger audit universe into a defined, budgeted, plan that can be delivered alongside additional requests from the AC and wider business.

A significant part of the complexity for audit leaders is trying to benchmark a draft plan and delivery approach amongst comparable peers and getting a broad sense of where you sit on the spectrum of possibilities.

We know, from deep experience, this is hard, and we want to help you.

Given our wide reach in the sector, we want to gather some helpful data from your peer Heads of Internal Audit with which you can benchmark. To keep matters as simple as possible, we have designed a short survey – just 5 questions - regarding the size of 2024 plans, resources and specialist skillsets expected to be used, data analytics and the biggest concerns on your agenda as an audit leader.

All survey responses will be anonymised, and we hope that with sufficient responses we can publish the results, and our analysis, in November's edition of this update.

The survey can be accessed on the following link:

IA Benchmarking Survey

The deadline for responses is 8 November.

We look forward to your response on our survey questions!

03

ESG UPDATE

TNFD RECOMMENDATIONS: WHAT DOES IT MEAN FOR THE FINANCIAL SERVICES SECTOR?

ADAM SOILLEUX
Associate Director

GLORIA PEREZ TORRES
Senior Manager

ESG UPDATE
TNFD recommendations

The publication of the Taskforce on Nature-related Financial Disclosures ("TNFD") Final Guidance for financial institutions on how to implement the TNFD recommendations sets out what banks, assets managers and owners, insurers and other financial services providers should consider to adhere to this initiative and when. Whilst this requirement is voluntary at the moment, a number of businesses are already adopting it with expectations of it becoming much more widespread in 2024 and 2025.

For firms seeking to follow this, this means that they need to be planning their disclosures now to start gathering the data.

WHAT IS THE TNFD FRAMEWORK?

The TNFD is a framework of 14 recommendations for 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.

In terms of metrics, however, there is an additional level of complexity as firms will need to consider assessment and disclosure metrics. Types of disclosure metrics include core global, core sector and additional metrics and should be reported on a 'comply or explain basis for those choosing to engage with the Framework voluntarily.

ESG UPDATE
TNFD recommendations

WHAT ARE THE IMPLICATIONS FOR THE FINANCIAL SERVICES SECTOR?

ESG expectations continue to evolve. Whether you decide to engage with TNFD now, or later, will be a business decision. In this context, early consideration may give firms a competitive advantage relative to peers. However, some firms may face challenges engaging with the framework in terms of resources, capacity, and costs.

Firms engaging early will need to review and update their ESG strategies and plans to be TNFD aligned. Other actions that firms should consider include:

- Developing an implementation framework;
- Identifying what reporting is going to look like;
- Assessing the resources, roles and skills that will be required within the second and third lines of defence assurance that will be required;
- Including an assurance review of the design of the implementation framework in the Internal Audit Plan.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

TNFD is currently a voluntary framework. However, firms can expect to be required to report on nature and biodiversity once the UK ratifies and incorporates the International Sustainability Standards Board (ISSB) Standards in UK regulations as it had been announced that TNFD Recommendations will inform the ISSB standards as they continue to develop.

Internal Audit will, therefore, need to check that the audit plan sufficiently covers the firm's data and reporting capabilities to support incoming disclosure expectations ahead of them becoming requirements.

04

CYBER RISK

BRAD DUFFELL-CANHAM
Director

CYBER RISK

Cyber Risk continues to be high on the agenda of Audit Committees and has, again, been reported as the top risk in the latest CIIA annual Risk in Focus survey. The consequences of a cyber-attack for organisations could be highly significant in terms of disruption to operations, inflicting reputational damage, theft or destruction of valuable or sensitive data, as well as the cost of fines by data regulators (and potentially ransoms paid to the hackers holding your data as hostage).

WEAPONISED CYBER ATTACKS

In 2022, the UK National Cyber Security Centre (NCSC) urged organisations to "bolster their cyber security resilience in response to the malicious cyber incidents in and around Ukraine" and published updated guidance. Reference was made to the destructive wiper malware which is being deployed against organisations in Ukraine and highlighting the risk that further attacks are likely to continue and may inadvertently spill over into organisations in other countries.

EMERGING TECHNOLOGIES & REGULATION

In the latest Risk in Focus, CAEs state that digital disruption, new technology and artificial intelligence (AI) will be their 4th biggest risk by 2027. AI offers organisations many new opportunities, but it can add complexity and new risk exposures. There are instances of AI being used to aid cyber-attacks. Combined with the broader "attack surfaces" created by cloud and mobile technologies, and increasing integration with business partners and suppliers, organisations will need to continue investing in their security capabilities.

New mandatory requirements are being set in EU legislation such as the Digital Operational Resilience Act (DORA), the NIS2 Directive, Data Act and Cyber Resilience Act.

PROTECT YOUR ORGANISATION

The NCSC guidance highlights the following good practices:

- **Patching is an essential protection and needs to be kept up to date.** Where attackers are seeking to exploit a known security vulnerability they move fast, and it is organisations with ineffective patching programmes that are most vulnerable.
- **The organisation needs to understand its Internet-facing footprint.** Vulnerability scans / penetration testing of the whole internet footprint need to be performed regularly to ensure that everything that needs to be patched has been covered. Know your "attack surface".
- **Access controls need to be checked carefully.** Extra focus should be applied to privileged or administrator access rights. Where possible multi-factor authentication (MFA) should be used and checked to confirm it is configured correctly. Third party access needs to be checked thoroughly, controlled and unnecessary access removed.

CYBER RISK

- **Anti-virus software and firewalls are important defences.** Antivirus should be active on all systems and updated correctly. Firewall rules must operate effectively.
- **Access to its backups is vital for an organisation to be able to recover its systems.** Backup routines must be running correctly, and any backup failures addressed. The ability to restore from backups should be regularly tested.
- **Mandatory training in cyber security needs to be provided regularly.** Unless reminded, individuals can forget the level of threat, the importance of staying alert and reporting phishing or other suspected attempts at intrusion promptly.
- **Logs must be configured and monitored**, leveraging Intrusion Detection (IDS), Intrusion Prevention (IPS) and Security Information Event Management (SIEM) systems to examine and monitor the events taking place in the network, including detection of potential threats and security policy violations.
- **Assume systems will be affected by a cyber-attack at some point.** Incident response plans need to be checked and tested so that the organisation can deal with an incident effectively. Playbooks should be established detailing the response to specific incident types.
- **The incident response team** also needs to be considered carefully so that individuals with the appropriate skills and authority to take meaningful decisions are available at very short notice, including third party dependencies and on-call arrangements with specialist suppliers.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

Critical information assets ("crown jewels") need to be well protected with defensive, monitoring and recovery controls strengthened as far as possible. Internal Audit should be looking at its audit plan once again to determine whether the assurance scheduled will be sufficient to meet the needs of the Audit Committee and the organisation during this period of heightened risk, rapidly emerging technologies and new regulations.

Internal Audit should also invest further in developing its skills and understanding of this important risk area so that it can engage across the three lines, including with its colleagues in Risk and IT security, and better explain the issues to the Audit Committee. Technical expertise on cyber is often sought from a co-source partner. Where this is the case, the internal audit team should look to work more closely with the partner team to build skills and maximise opportunities for knowledge sharing.

05

ECONOMIC CRIME UPDATE

SONIA DOHIL
Manager

ECONOMIC CRIME UPDATE

SANCTIONS SYSTEMS AND CONTROLS: FIRMS' RESPONSE TO INCREASED SANCTIONS DUE TO RUSSIA'S INVASION OF UKRAINE

On 6 September the Financial Conduct Authority ("FCA") set out key findings from its assessments of sanctions systems and controls in financial services firms. This included examples of good practice and areas for improvement, to help firms deliver even greater compliance with sanctions.

The unprecedented size, scale, and complexity of sanctions imposed by the UK Government and international partners since Russia's invasion of Ukraine, has further increased the FCA's focus on firms' sanctions systems and controls.

The FCA assessed sanctions controls for over 90 firms across a range of sectors including retail banking, wholesale banking, wealth management, insurance, electronic money, and payments, to ensure firms' financial sanctions systems and controls are:

- adequate and effective at addressing sanctions risk and
- appropriate to respond swiftly to changes in UK sanctions regimes.

This is relevant to all banks and building societies and their Money Laundering Reporting Officers, Nominated Officers and teams working in financial crime compliance roles.

The FCA identified areas of good practice and where firms need to make improvements in, notable in the following areas:

- Governance and oversight
- Skills and resources
- Screening capabilities
- Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures
- Reporting breaches to the FCA

Where the FCA identifies issues with firms' systems and controls in the above areas, feedback is being provided and, in some circumstances, regulatory tools used to remedy issues. Tools may include, but are not limited to, the use of independent skilled persons and interventions such as imposing business restrictions on firms or enforcement action where serious misconduct is identified.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

Banks and Building Societies should continue to evaluate their approach to identifying and assessing the sanctions risks they are exposed to and actively strengthen their measures to prevent sanctions breaches and evasion, adapting to the evolving sanctions landscape and changing risk exposures.

The FCA identified a number of findings under five key themes, therefore focus should be given to the following elements of firms Financial Crime frameworks:

Governance and oversight

- Ensuring there is regular monitoring and review of the effectiveness of sanctions through sufficient management information;
- Sanction reporting and policies are calibrated and aligned to the UK regime.

Skills and Resources

- Ensuring proper resourcing of sanctions teams to avoid backlogs in dealing with sanction alerts and enable quick reactions to sanctions risks.

Screening Capabilities

- Ensuring screening tools are appropriate for the UK sanctions regime and calibrated to the specific risks the firm faces.

Customer Due Diligence (CDD) and Know Your Customer (KYC) procedures

- Maintaining effective and high-quality CDD and KYC assessments, and backlogs are addressed in a timely manner.

Reporting breaches to the FCA

- Ensure that any identified breaches are reported in a timely manner and with accuracy to the FCA on potential sanction breaches.

The FCA expects banks and building societies to consider its findings, evaluate their approach to sanctions risk and take actions where appropriate. As well as this, banks and building societies should engage with the FCA in testing and report any significant deficiencies identified.

ECONOMIC CRIME UPDATE

FCA LAUNCHES REVIEW INTO HOW FIRMS ARE HANDLING POLITICALLY EXPOSED PERSONS

On 5 September the FCA set out its approach on its review of the treatment of domestic Politically Exposed Persons (PEPs) by financial services firms following recent complaints of unfair treatment by a high-profile figure over the summer.

The FCA's review will look carefully at firms' arrangements for dealing with PEPs based in the UK. While the FCA cannot change the law in place for the PEPs regime, it will take prompt action if any significant deficiencies are identified in the arrangements of any of the firms assessed. The FCA has already requested policies and procedures from a number of firms and have reached out to UK politicians, such as senior civil servants and MPs, on their treatment by the financial services industry.

The review will be completed and reported on by the end of June 2024.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

Banks and Building Societies should be prepared for a possible review by the FCA on the following:

- Their approach to applying the definition of PEPs to individuals;
- Whether there are proportionate risk assessments of UK PEPs, their family members and known close associates;
- The application of enhanced due diligence and ongoing monitoring is proportionate and in line with the risk appetite;
- Clear documentation of decisions to reject or close accounts for PEPs, their family members and known close associates;
- Clear documentation of pertinent communications with PEP customers;
- Keep PEP controls under review to ensure they remain risk-based and proportionate.

HM TREASURY: FROZEN ASSETS REPORTING – OFSI PUBLISHES 2023 REPORTING NOTICE

On the 7 September, the Office of Financial Sanctions Implementation (OFSI) published its frozen assets reporting notice, which requests, firms that hold, or control funds or economic resources belonging to, owned, held, or controlled by a designated person, to provide a report to them with the details of these assets.

Most UK financial sanctions regimes are implemented through the Sanctions and Anti-Money Laundering Act 2018 (SAMLA). The SAMLA provides OFSI with the powers to request data as part of its remit for monitoring compliance with the legislation. As part of its monitoring oversight, OFSI undertakes this review to update its records to reflect any changes to frozen assets held by firms during the reporting period.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

Banks and Building Societies should ensure that:

- They identify all reportable assets, data held on individuals and entities with funds or economic resources frozen in the UK as well as those overseas (if they are subject to UK financial sanctions legislation) is up to date and easily accessible.
- They have a dedicated individual responsible for collating and sending in the return to avoid duplication of information.
- Data is accurate as at 29 September 2023 and is submitted by the 10 November 2023

The obligation to report as part of OFSIs annual review is separate to the mandatory obligation for firms to report to the OFSI on any sanction hits and breaches that they identify. All newly frozen funds or economic resources must be reported immediately.

For further detail, please refer to the Financial Sanctions notice.

THE FCA HAS PUBLISHED THE FINDINGS OF ITS INITIAL REVIEW ON BANK ACCOUNT ACCESS AND CLOSURES

On the 19 September, the FCA set out their initial findings on bank account access and closures. The data provided by firms indicated the most common reasons for account closures were dormancy/inactivity or concern the account was being used to further financial crime, both within the law and FCA rules.

The FCA did not find any evidence to suggest that firms had closed any accounts between July 2022 and June 2023 primarily because of a customer's political views.

To better understand the scale and reasons for any account closures, the FCA gathered data from 34 firms on the:

- number of accounts terminated
- number of accounts suspended

ECONOMIC CRIME UPDATE

- number and type of consumers declined accounts
- reasons for these decisions and
- complaints received on this issue

This was directed at Banks, Building Societies and Payment institutions.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

The FCA expects firms to draw on the findings set out in their report and reflect on actions they should take.

In the first instance firms should ensure that they have a clear framework, systems and controls on account closures, with focus on the following:

Management Information

- Ensuring that there is adequate monitoring of the nature, scale and impact of account declines, suspensions and terminations;
- Ensuring there is focus on customer outcomes and subsequent actions, including whether any distinct groups (e.g., vulnerable and protected customers) are receiving worse outcomes.

Data Accuracy

- Ensuring there is focus on the accuracy of data being reported.

Closing of accounts for political beliefs or opinions

- Be prepared for analysis of conclusions reached on accounts closed for political beliefs or views lawfully expressed;
- Ensuring there is consistency maintained around reasoning of account closures due to reputational risk, with clear criterion and evidence of how this is being used.

Declining Applications

- Firms should be prepared for reviews of declined applications and terminations of basic bank accounts.

Additional work by the FCA is expected to better understand the reasons behind, for example, the closure of accounts due to reputational risk.

FOR MORE INFORMATION:

RICHARD WEIGHELL
Partner

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

www.bdo.co.uk

42020160