INTERNAL AUDIT SUPPORT

BANKING & BUILDING SOCIETIES

June 2023

IDEAS | PEOPLE | TRUST

BDO

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 June 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

2023 REGULATORY PRIORITIES

2023 REGULATORY PRIORITIES

PRA 'Dear CEO' letter for Deposit-takers

REGULATOR	SECTOR RISK	PRA FOCUS
Credit Risk	The impact of increasing interest rates, inflation and high cost of living, geo-political uncertainty, and supply chain disruptions is expected to pose challenges to firms' credit portfolios. In recent years, firms have tightened underwriting standards, enhanced forbearance tools and increased operational preparedness for collections. However, these enhancements are untested under the current combination of risk factors.	Focus will centre on higher risk areas including retail credit card portfolios, unsecured personal loans, leveraged lending, commercial real estate, buy-to-let and lending to SMEs. The PRA will review firms' early warning indicator frameworks and make requests for enhanced data and analysis.
Financial Resilience	The PRA expects firms to take proactive steps to assess the implications of the evolving economic outlook on the sustainability of their business models. This should include consideration of broader structural changes, such as the evolution of new financial technology and competition.	The PRA will continue ongoing assessment of individual firms' capital and liquidity positions as well as how these June evolve in light of potential headwinds. Areas of focus will include the impact of evolving retail and wholesale funding conditions, as well as scheduled maturities of drawings from the Term Funding Scheme in the coming years. Supervisors will continue to work with firms as they seek to enhance their own testing and scenario development capabilities in response to the current environment.
Risk Management & Governance	The default of Archegos Capital Management and recent market volatility from the Russia/Ukraine conflict have shown that firms continue to unintentionally accrue large and concentrated exposures to single counterparties, without fully understanding the risks that could arise.	PRA will continue to assess firms' risk management and control frameworks through individual and cross-firm thematic reviews. Regulatory supervisors will focus on firms' ability to monitor and manage counterparty exposures, particularly to non-bank financial institutions. Given the global nature of market events, the PRA will continue to work closely with its global regulatory counterparts on these topics.
Operational Risk & Resilience	In response to increasing digitisation, changes in payment systems and the need to address legacy IT systems, many firms are executing large and complex programmes of IT change. There has been a material increase in services being outsourced, particularly to cloud providers, and the number of firms offering crypto products continues to grow, presenting new challenges for risk management.	The PRA will continue assessment of firms against the operational resilience requirements, firms' own self-assessments, and the testing that firms are conducting. The PRA also expects large-scale IT changes to be well managed with the associated transition and execution risks appropriately mitigated, outsourcing arrangements to meet the expectations on outsourcing and third-party risk management. Focus will include firms' use of new technologies, and advancements in asset tokenisation as firms are expected to have fully understood the impact of offering crypto products on their operational resilience.

2023 REGULATORY PRIORITIES

PRA 'Dear CEO' letter for Deposit-takers

REGULATOR	SECTOR RISK	PRA FOCUS
Model Risk	The weaknesses that the PRA highlighted in its 2022 priorities letter for Model Risk Management (MRM) remain a priority.	The PRA expects to publish finalised MRM principles for banks in H1 2023. For Internal Ratings Based models, the regulator will continue to focus on three key workstreams: the implementation of IRB Hybrid mortgage models; the IRB Roadmap for non-mortgage portfolios; and IRB aspirant firm model applications. Focus will include new Fundamental Review of Trading Book (FRTB) models and firms' intended methodologies.
Regulatory Reporting	Repeatedly identified deficiencies in the controls over data, governance, systems, and production controls related to regulatory reporting.	The PRA expects firms to consider the thematic findings set out in its communications on regulatory reporting to help improve future submission and the regulator will continue to use skilled person reviews in this area in 2023.
Climate Change	The level of embeddedness of PRA climate change financial risk requirements (PRA SS3/19) varies across firms.	The PRA expects firms to take a proactive and proportionate approach to addressing risks in this area as set out in its most recent Dear CEO letter.
Diversity, Equity & Inclusion	A new consultation paper expected this year setting out proposals to introduce a new regulatory framework on DEI in the financial sector.	
Resolution	Firms need to continue to ensure that they achieve, and can continue to maintain, the resolvability outcomes of the Resolvability Assessment Framework, and ensure that they are transparent in their disclosures about their preparations for resolution.	

02

MEET THE TEAM

MICK CAMPBELL
Partner, 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 Mick Campbell.

1. What has been your career leading into BDO?

I joined a Big 4 firm in 2001 in its financial services (FS) risk advisory team and worked on a range of risk and regulatory related engagements across insurance firms, asset managers, retail banks and investment banks. After six years, I moved into another Big 4 firm to help establish and grow its FS risk advisory team within Scotland. During my 13 years with the firm, I led a wide variety of clients and engagements in Scotland, across the UK and internationally.

In 2019, I joined a prominent FS outsourced services firm to lead its second line of defence for its FCA-regulated entity. The switch from consulting to a role in industry enabled me to build on my experience and provided a broad range of exposure to operating at Executive and Board level, dealing with regulators and overseeing major transformation and re-platforming programmes.

I joined BDO in February 2023 to establish and lead our FS Advisory team and services in Scotland and support our strategic aims across the UK. I have really enjoyed my first four months at BDO, meeting people across the business and (re)connecting with clients and I'm looking forward to building the team and supporting our clients in Scotland and across the UK!

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

My role is varied, as I support growth of our FS Internal Audit and Advisory teams:

- I lead a portfolio of Internal Audit engagements, supporting clients in either outsourced or co-sourced internal audit across the FS sector;
- Developing our financial services risk management and regulation offerings, with a focus on enterprise risk management, risk governance and risk culture;
- Leading Skilled Person engagements, or supporting clients with preparations for Skilled Person reviews, where the focus is governance, risk management and / or regulatory compliance and effectiveness;
- Supporting BDO's internal Quality and Risk processes by acting as a sounding board for client take-on, due diligence, etc.;
- Working with other senior leaders in BDO to grow our insurance sector team and market offering.

I enjoy working with clients and supporting achievement of their strategic objectives. As advisers, it is essential we add value through our insight and experience to ensure client objectives are met, whether they be organisational or personal objectives for our stakeholders.

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

Having recently joined BDO, my focus has been on meeting people across the UK firm and other international member firms to understand the wide range of experience and capabilities we have at BDO and I have been hugely impressed! I have been involved in number of interesting proposals recently, covering internal audit, third party assurance and governance effectiveness. One proposal related to supporting a client with enhancing their finance function operating model and associated processes. This involved working across several teams within BDO to ensure our team and approach was the best offering to the client.

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

The best thing so far has been how welcoming everyone has been to me since I joined the firm. There is a strong culture of collaboration, and this has been demonstrated in everyone that I have met. The team has a wide and diverse range of backgrounds, experiences and technical capabilities and this helps us all work together and learn from each other. It also helps us to offer our clients a distinctive service and have some fun while doing so!

5. What drives you to do what you do?

Being part of a business that is growing, and having responsibility for contributing to that growth, is very motivational for me. My family also inspires me to keep improving and learning and this role enables that.

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

My career path has not been a linear progression and there have been setbacks on the way. One thing that has surprised me is the importance of resilience as it has helped me to learn, grow and bounce back!

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

Be yourself.

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

I think everyone is already thinking about how AI will impact business, what we do on a day-to-day basis across our lives, and internal audit is no different. Change is already happening and internal audit, along with other disciplines and the general way of doing business, will need to evolve rapidly to keep up.

My personal opinion is that I expect governments and regulators will be looking to seize the opportunities AI provides while also developing guidelines and regulation. The extent to which this can keep pace with the speed of AI development, and be applied effectively, remains to be seen.

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

I like playing golf and watching football and most other sports. I enjoy running and try to get out before the working day starts.

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

Sunscreen, sunglasses and a jet ski!

03

TRANSFORMATION RISK AND COORDINATED ASSURANCE

MICK CAMPBELL
Partner, Financial Services Advisory

TRANSFORMATION RISK AND COORDINATED ASSURANCE

In this article, I build upon the insight from my colleague, Richard Weighell, regarding Transformation risks relevant for internal audit teams, published in September 2022, to share thoughts on the industry trends and experiences that I have gathered during my career. We will specifically discuss the two subjects which are common areas of challenge for financial services firms – and typically areas internal audit functions are requested to review:

1. **Transformation Risk; and**
2. **Three lines of defence model, specifically, how firms effectively allocate role and responsibilities across the three lines of defence to manage, monitor and review transformation risk.**

What is Transformation Risk?

Transformation risk is the risk associated with failure to deliver transformation activities in accordance with the budgeted time, cost and quality standards to the extent it may result in disruption to business operations, customer service, failure to meet strategic objectives, failure to meet the overall business case and may also result in reputational damage to the firm.

"Transformation" itself can be any activity for an organisation that is deemed material enough to transform, change, enhance and improve the current way of working. For example, this could be a customer services telephony system replacement and process engineering for a firm's customer contact centre, or it could be a major system replacement for an organisation who is seeking to replace legacy IT infrastructure to improve efficiency and enhance resilience of its operation. Materiality is typically defined by the organisation and is usually driven by cost, benefits to be derived from the programme and risk associated with delivery.

What are the roles and responsibilities of each of the three lines of defence?

Some organisations have found defining a structured, coordinated, approach to the oversight of programme risk can provide assurance to key stakeholders, such as Programme Steering Committees, Executive Committees and Boards, on the effective management of inherent risks to transformation programmes.

When defining detailed roles and responsibilities it is important to clarify and document the high-level responsibilities of each line of defence. For example:

TRANSFORMATION RISK AND COORDINATED ASSURANCE

1st line - Programme

- Maintain control and effective risk management across the programme through adoption of a consistent programme methodology and clear accountability for risk ownership and management;
- Perform self-review through continuous challenge, oversight and governance reporting of the programme risk profile. The approach should not be seen as an overhead, but an integral part of managing change and its related risks.

2nd line - Risk Function - Programme

- Define and document approach of the independent second line of defence activities across the programme;
- Split responsibilities by 'advisory' and 'assurance' activities. For example, advisory activities can include attending key working groups, decision fora, committees etc. to represent and contribute the second line of defence opinion. Assurance activities, can include performing thematic reviews as agreed with the Board, Exco and CRO with formal reporting output distinct from internal reviews;
- Compliance monitoring plan may include a review of transformation activities affecting, or likely to affect, the compliance risk universe.

3rd line - Internal Audit

- Define and deliver an internal audit plan over the transformation programme, approved by the Audit Committee;
- May include engaging with co-source partners for access to specific skill sets where appropriate.

Delivering effective and co-ordinated assurance over transformation programmes

Transformation programmes are inherently complex, costly and risky and they often fail to deliver within planned timescales, budgets or planned benefits. However, when they deliver, there can be benefits for customers in the form of a better service, for employees in the form of improved ways of working, as well as longer-term risk profile and financial benefits.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

IA teams should first consider the common obstacles to implementing effective and co-ordinated assurance activities across complex programmes of activity such as:

- **Assurance and oversight of the risk profile is seen as the job of the risk function and/or internal audit**: Programme budgets should ensure there is a proportion allocated to first line resource to support embedding of risk and control management within the programme. If this is absent, there will be additional cost to budgets and/or delays to delivery timelines as resources intended to support delivery may need to be reallocated to other activities to deliver effective programme risk management. There needs to be clear accountability for delivery of programme risk management for this to work.
- **Assurance providers do not co-ordinate activities resulting in multiple reviews targeting the same areas or missing key areas of risk due to lack of clarity of scope coverage**: It is essential assurance providers coordinate their plans and delivery activities to mitigate this risk. This can include stakeholders such as Programme Leadership, PMO, first line risk, second line risk and compliance, internal audit and external assurance providers meeting to share and agree planned activities, and then convening on a frequent basis to share key findings and recommendations from reviews. The stakeholder matrix can be complex across transformation programmes, it is, therefore, essential there is regular sharing and discussion of assurance activities and their output at formal governance meetings.
- **Reporting is extensive and stakeholders can feel overwhelmed with detail**: This is a common pitfall – as noted previously, these programmes can be complex, costly and risky. Subsequently, there can, on occasion, be a tendency for assurance providers to ensure their review passes the 'weight test', i.e., it is lengthy enough to justify the amount of time and budget spent on the review. Assurance providers need to ensure their findings and recommendations are provided in the context of the programme risk profile and actions are rated by priority and complexity as this will help stakeholders conclude where they need to focus attention to resolve issues.

04

ESG UPDATE

ESG MATURITY FOR BANKS AND BUILDING SOCIETIES

ADAM SOILLEUX
Associate Director

GLORIA PEREZ TORRES
Senior Manager

ESG MATURITY FOR BANKS AND BUILDING SOCIETIES

The sector faces escalating climate risks that can be physical, directly affecting the business, or transitional, affecting credit portfolios through volatility in asset prices. There is also the risk of greenwashing that arises from products and services that are offered as "green" or "sustainable" but, in reality, are not. This, together with mounting pressure from shareholders and clients on the banking sector to support the economy's transition to net-zero, has resulted in increased regulatory requirements and stakeholder expectations.

Climate change and ESG maturity for banks and building societies

ESG, sustainability obligations and expectations are evolving fast in the financial services sector. Initially, in April 2019, the PRA's Supervisory Statement 3/19 required banks to manage climate risks and to consider reporting in line with the TCFD recommendations. More recently, regulators extended the scope to cover diversity and inclusion and, in 2022, the FCA's Policy Statement 22/3 mandated listed banks to set out specific diversity targets, report on them and further plans to expand on diversity governance requirements for the sector were announced by the FCA in their Discussion Papers published in 2021 (FCA DP 21/3) and 2023 (FCA DP 23/1).

There is a lot to keep up with and this has an impact on how 'mature' a control framework is. Moreover, the level of ESG maturity is closely linked to the firm's business strategy, ambition, and vision. However, regardless of the initial ambition, there will be a desired current position where every organization will want to meet the new minimal regulatory and disclosure requirements.

Larger banks with relatively more resources may have an ESG driven culture. However, those with a vision to seek opportunities or those committed to ESG will eventually catch up as they see the benefits that more advanced ESG and sustainability programmes will bring to business value. In our experience, climate and ESG maturity is a journey rather than an end in itself, where firms continuously improve their programmes.

The graph below shows how we at BDO calibrate the maturity position and journey for firms:

ESG MATURITY FOR BANKS AND BUILDING SOCIETIES

Why does ESG maturity matter?

Boards are responsible for driving their firm's ESG strategy and the firm's ESG maturity. To a large extent, how Boards respond to these new requirements depends on their attitude to ESG and its incentives.

Whilst resources, costs, and business pressures present challenges to developing maturity, it also presents opportunities and there are a number of reasons why it should matter to senior management teams:

- ESG increasingly matters to investors, employees, as well as the wider public perception of the firm's brand on key topics, such as carbon footprint and investment to alleviate local community issues. Clients will avoid engaging with firms that fail to exhibit a mature ESG mindset and approach to culture;
- Regulators expect Boards to be able to demonstrate an ability to understand and effectively manage ESG risks;
- ESG maturity can provide firms with a competitive advantage in the marketplace. Research shows that well-developed ESG programmes can help to facilitate top-line growth, reduce costs, minimize regulatory and legal interventions, increase employee productivity, and optimize investment and capital expenditures (McKinsey 2019). However, whilst credit institutions are generally more advanced in their climate risk management frameworks, as a consequence of regulatory and stakeholder expectations, their wider ESG considerations are still a work-in-progress and it is the role of Internal Audit to appropriately track the firm's ESG maturity and assure that ESG risks are being managed effectively within risk appetite.

What should Internal Audit teams think about?

Internal audit plays a pivotal role in providing meaningful assurance to the board and senior management on its controls for climate change and ESG risks. The IA function will also be sought for assurance on the effectiveness of second-line teams that have to deal with the increasing regulatory and stakeholder expectations associated with ESG risks.

Our experience in the market has shown us that banks and building societies have an established track record in modelling long-term risk; however, internal audit teams should be aware that climate and sustainability knowledge, skills and experience continue to pose a material challenge for the sector.

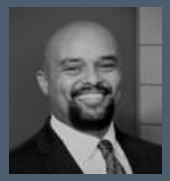
The ESG landscape is evolving at a rapid pace, and this sometimes requires additional resources with specialist skills to provide timely advice, guidance, market benchmarking and gap analysis against regulatory expectations to help third-line assurance providers keep up with the pace. If you have any questions, please contact a member of BDO's Financial Services ESG team.

05

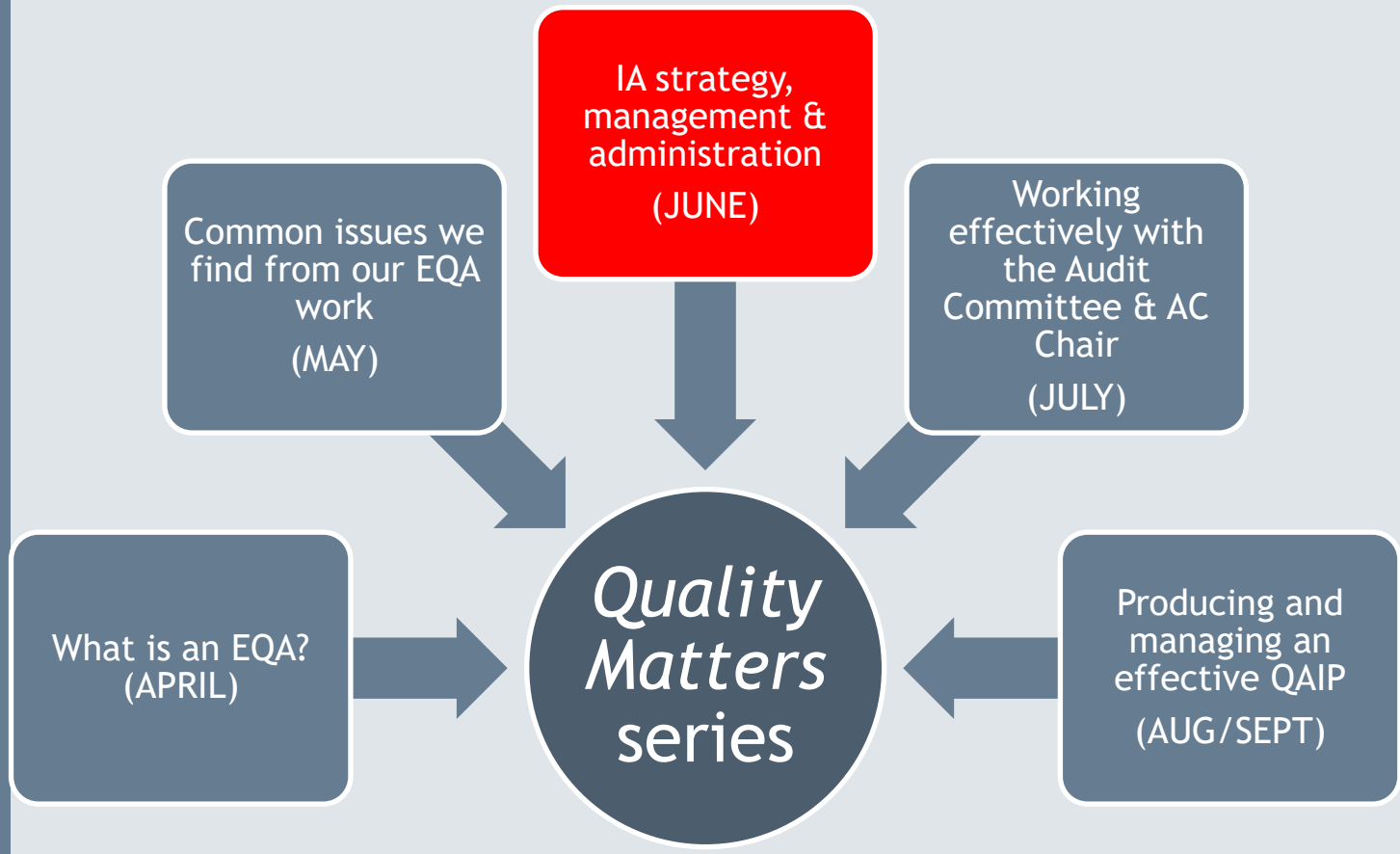
QUALITY MATTERS
PART 3

IA STRATEGY, MANAGEMENT & ADMINISTRATION

SAM PATEL
Partner



BRUK WOLDEGABREIL
Associate Director



QUALITY MATTERS – PART 3

IA strategy, management and administration

In our May pack, we explored the common challenges and issues we've observed from our External Quality Assessments (EQA), as well as our insights on matters arising from a general Internal Audit (IA) perspective and not linked to a specific aspect of the guidance or standards.

This month, we delve deeper into the IA strategy, management and administration findings we've typically picked up on from our EQA engagements.

While most IA functions have a sensible strategy and good working relationship with the first and second lines, as well as the statutory (external) auditors, there are often some simple good practices missing within strategy setting and the key administrative matters, such as demonstrating independence, that hold the IA team back from achieving its full potential.

STRATEGY AND VISION

In some IA functions we have worked with, the Head of Internal Audit (HoIA) has incorrectly interpreted the IA Charter as the IA function's strategy. The IA Charter is vital to enshrine the function's position in the firm and its authority to access the firm's records, personnel, and physical assets; but it is not a strategy document.

If we start from the CIIA's Technical Guidance for "Auditing Strategy", we can best understand "organisational strategy" as how the firm will want to move from where it is now to where it wants to be. Underpinning that strategy would be a set of clearly defined objectives to help move the firm to its aspired destination, which comprise the firm's:

- Mission - what the firm wants to achieve today;
- Vision - what the firm wants to achieve or become in the future; and
- Actions - what the firm will have to do to get there (firm objectives, targets, goals etc.).

The IA function's strategy needs to be a reflection of the firm's strategy so that priority risks are assured and organisational value is enhanced, best articulated as the IPPF's Mission of Internal Audit:

"To enhance and protect organisational value by providing risk-based and objective assurance, advice and insight."

The Mission should include the IA Charter (effectively, IA's badge of authority), the annual audit plan approved by the Audit Committee (AC), the IIA standards, guidance and FS Code with which to undertake internal audit work. So once an IA function is clear on its Mission, its needs an articulation of its Vision and the actions required to move the function to its aspired position.

Let's start with Vision for the IA function. The HoIA should have a good sense for where they would want their function to be by the end of this annual plan, by the end of the 36-month cycle and a broad idea of what the function could look like in five years' time. This is not about achieving the plan of audit reviews, rather this is a consideration of how the IA function needs to be fit now for future risks (and opportunities) and from our assessment work this should include IA's:

- **Purpose** – what will be the purpose of Internal Audit in the future? Increasingly, control functions in the second line are professionalising their assurance activities, goaded on by increased regulation and the growing expectations from senior management for cost functions to better demonstrate their "value add". This could potentially leave the IA function squeezed into a thin peripheral layer coating the various control reviews and testing undertaken by Compliance, Risk, Finance, Legal, etc. The HoIA needs to differentiate and define the IA function's purpose based on the uniquely objective and independent standpoint that it has relative to other teams and maintain this visibility on a continuous basis by drawing unparalleled insight from its assurance activities. **The IA's assurance activities should therefore be a means, not an end, for IA to add value into the firm**. Underpinning this meaningful purpose is the HoIA regularly and proactively speaking with the AC Chair, Board, senior management, and client-facing teams on what they would wish for from the IA function to help make the firm's clients happier and business teams more efficiently achieve the firm's objectives. We don't always see this in some IA functions, and this typically leads to IA being perceived as "siloed", bureaucratic, fading into the background and forgotten about when the firm's strategic discussions take place. Such views tend to come through in EQA surveys or interviews with senior managers about their perception of the IA function and its value to the firm;

QUALITY MATTERS – PART 3

IA strategy, management and administration

- **Technology** – we are living through a transformational period in which national governments are having to debate whether the full potential of artificial intelligence should be unleashed. For the Internal Audit function, if there is not now an active debate as to how newly released open access tools will impact day-to-day operations over the next five years, e.g., GPT 4 to deliver the majority of report writing, then the option to consider this development will soon be taken out of the HoIA's hands by the firm's own strategic realignment to incorporate deep learning technology. IA needs to at least document a SWOT analysis for how incoming technological advancements, including full digitalisation of the IA function, could impact IA operations. A lot of firms have already been developing power BI reporting – is this already a thing of the past?;
- **Resources** – thinking about the quantum and quality of technical skills the IA function will need over the next five years is difficult as it would be premised on the anticipated technology, purpose of the IA function and the business risks which the firm forecasts on the horizon that need to be assured by the IA function. There is no one-size fits all approach as Resourcing requires its own strategy, which we have covered extensively in our March Pack;
- **Quality Assurance** - an effective Quality Assurance and Improvement Programme (QAIP) today will support the IA function's internal growth as a value-accretive component of the firm's control environment. The evolution that the IA function should now consider is taking its specialist skill for self-assessing, monitoring and enhancing quality factors to proactively offer other teams across the wider firm the opportunity to learn from IA on how they can develop their own QAIP and, thereby, elevate IA's role as a "Quality Champion" for the whole firm (not just its own IA function). While the current practice is for IA to facilitate a department's Risk and Control Self-Assessment, the future will likely place IA's advanced skillset for quality assurance as an educational asset to coach business teams to most effectively work with the outputs they draw out from their technology-based continuous risk monitoring systems in the near future (they will soon arrive, if not already here in some larger or technology centric firms).

Documenting the IA function's strategy is likely to be more straightforward. The CIIA have provided Technical Guidance ("Writing an Internal Audit Strategy") so that IA functions can follow the procedural steps to help bring out the future fit considerations explored above; the most important of which being consultation with a wide variety of stakeholders to help incorporate the expectations of senior management, the Board and heads of business teams. You would be surprised at how many EQAs we've delivered whereby the HoIA hasn't asked their key stakeholders what they want from IA. Just because they say it, doesn't mean it has to be done – but at least expectations are then rationalised.

Once a coherent strategy is in place for the IA function, the IIA's Supplemental Guidance – "Developing the Internal Audit Strategic Plan" – is a helpful resource to consider the common triggers for a review of the IA function's strategic plan. The IA function's strategic plan should be a dynamic document if it's to achieve its intended purpose and, therefore, needs to be revisited frequently to align with:

- the firm's review of its strategic plan;
- significant impact on the IA's resourcing strategy (e.g., merger or business disposal);
- significant changes to the firm's applicable regulatory framework (you may remember the years of preparation for Brexit?);
- leadership changes at the Board level; and
- recommendations following an EQA.

QUALITY MATTERS – PART 3

IA strategy, management and administration

INDEPENDENCE

Independence is at the core of the IA function's mission and should be incorporated into the IA's regular administration activities. However, once independence requirements are documented in the IA Charter, we have found in some functions that independence typically receives a superficial review (if at all) on an annual basis and not much more is discussed about it thereafter.

Independence needs to be considered on an organisational basis for the function (AS 1110 – Organisational Independence) and for individual auditors (AS 1120 – Individual Objectivity); the issue we come across more often is that the independence of the HoIA and members of the IA function's senior management that have been with the firm for a considerable amount of time are not proactively examined for any perceived impairments to independence on a periodic basis or challenged on certain assurance engagements where reviews of an auditable entity are routinely carried out by the same auditor. The risks from an impairment to independence or objectivity do not generally leap out at a point in time; they tend to creep in slowly over time if left unchecked.

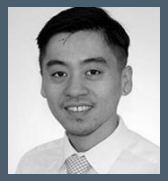
Our assessment work has consistently shown us that effective IA functions put sufficient efforts in place to proactively maintain independence, for example, through rotating cyclical audits across different team members so that the team's familiarity with a business area is mitigated. Well run functions also tend to document independence on a regular basis, either on a semi-annual basis to assess individual auditors for potential conflicts that crop up in the audit cycle (e.g., a work-based relationship between an IA colleague and a team member from a business team is recorded by HR), or more routinely by establishing an independence workbook for each engagement to collate independence attestations from each auditor to be involved in an assignment. The method to maintain and document independence will need to be proportionate to the size and complexity of the IA function, but it needs to be demonstrable to evidence that the independence and objectivity obligations of the function agreed to in the Charter are being adhered.

With respect to the organisational independence of IA functions in smaller firms, the central issue we have found is the IA team being drawn into first- and second-line activities. It's a difficult balancing act, but IA functions at the very edge of independence can only facilitate, not participate, in the activities for which they will need to assure. A helpful tool to demarcate IA's sphere of activities is an Assurance Map to articulate what each assurance provider is responsible for and where IA's specific input will be expected by the AC. We generally see some form of assurance planning between IA, second- and first-line teams, but it's not always documented in one place and, when it is documented, it's not routinely reassessed alongside changes to the IA strategic plan, annual audit plan, internal reorganisation of the firm or made sufficiently visible to senior management on a periodic basis.

We look forward to sharing the next instalment of our "Quality Matters" series in July where we explore ways of working effectively with the Audit Committee and its Chair based on insights gathered from our EQA and quality assurance work.

06

DEVELOPMENTS IN MODEL GOVERNANCE



KEVIN ZHANG
Manager

DEVELOPMENTS IN MODEL GOVERNANCE

WHAT'S NEW?

In 2018, the PRA initially set out its expectation as to the model risk management practices firms should adopt when using stress test models (Model risk management principles for stress testing – PRA SS3/18). The regulator further issued a Consultation Paper (Model risk management principles for banks - CP6/22) in June 2022, which proposed the PRA's expectations regarding banks' management of model risk.

More recently, on 17 May 2023, the PRA published its policy statement (Model risk management principles for banks – PS6/23), which provides the regulator's feedback to the responses received on last year's consultation.

This article will explore what model risk management is and what the recent developments mean to all PRA-regulated firms.

WHAT IS MODEL RISK MANAGEMENT?

As the name suggests, model risk management is the management of risks related the use of a model. To avoid being autological, a basic definition of a "model" is needed. Albeit this is more problematic than one would expect.

The PRA, quite broadly, defines a model in CP6/22 as a "quantitative method that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into output."

Frankly, this could apply to any Excel formulae used by the business.

The reality is that models used by businesses extend to a wide array of purposes and formats, from manual Excel driven spreadsheets to complex automated system-built models entailing a library of input and data sources.

As such, the firm needs to understand that the risks of each model vary depending on its format and complexity, and the management of those risks must be tailored to be effective and proportionate in the eyes of the regulator.

WHY IS IT IMPORTANT AND WHY YOU SHOULD PRIORITISE THIS ISSUE?

Easy answer – it's unambiguously listed on the PRA's 2023 priorities in its Dear CEO letter published earlier this year.

More nuanced answer - given the sector's increasing reliance on data for information and models for decision-making, the recent regulatory activity in this area is sufficient evidence to suggest firms should expect increased scrutiny over the course of this year and into 2024.

While the PRA's recent policy statement is explicitly aimed at UK-incorporated banks, building societies, and PRA-designated investment firms, some core risks extend beyond this scope. For example:

- Governance – models should have sufficient governance and oversight from stakeholders.
- Model validation – models function as intended.
- Model accuracy – model output(s) is accurate.
- Data integrity – data sources and model inputs are reliable.
- Model revision – revisions, updates or changes follow an appropriate governance process.
- Access and storage – models are stored securely and only intended authorised users have access.
- We should not be surprised if the FCA soon adopts a similar, proportionate, aim for its own supervisory approach to model risk management.

VALUE

Models are assets to a firm. Firms rely on models to make strategic and operational decisions. Having a robust model risk management framework in place means:

- **Effective risk management**: good model risk management practices can help avoid misguided decision making that leads to potentially catastrophic consequences, including financial losses, customer detriment and inappropriate discharge of Board responsibilities.
- **Operational efficiency**: model inaccuracies typically drive suboptimal monetary strategies. Mature frameworks can safeguard against this to support cost reductions and better capital allocation.
- **Regulatory comfort**: assuring the regulator on the firm's model risk management early on can enhance the PRA's overall confidence in the firm and forestall increased scrutiny and regulatory costs.

DEVELOPMENTS IN MODEL GOVERNANCE

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

Start from getting the basics right.

Is there a consistently understood definition of a "model" within the firm and have teams comprehensively identified all models in scope of that definition?

- Despite the PRA's definition of a model, we generally come across firms that are still unclear as to what constitutes a model or what should be in scope of the firm's Model Risk Management Framework.
- Another challenge is the consideration of model inputs. Some firms have various input sources for a model and those inputs can be considered models themselves. As a result, many model inventories are either over-subscribed or under-subscribed.

Is the model risk management framework pragmatic and how does the business assess proportionality of risks?

- Far too often, we see model risk management frameworks articulate control environments that are either impractical or do not sufficiently consider the specific characteristics of the models. Models can be simple or complex, built in-house, bought "off the shelf" or externally provided and maintained by a vendor – each with different risk profiles and maintenance criteria that require relevant and considered controls.
- Models can also be used across various departments with different processes. Firms need to be clear on the difference between model risk management principles and utility, as well as the type of audit review that should be deployed (e.g., end-to-end audits) to evaluate management of risks for a model that potentially straddles multiple business units.

Is there tangible buy-in from the senior management and Board?

- More often than not, firms see model risk management as another set of very technical, perhaps esoteric, prudential requirements layered on top of an already heavy regulatory burden. While Boards and senior management may ostensibly recognise the risks, it is down to the first line end users to identify, mitigate and manage those risks – if the tone from the top does not clearly communicate the priority of model risk management to the firm, then it's almost inevitable that model governance across the firm will be deficient for most of the regulatory expectations and it's only a matter of time until the firm's next PSM or inclusion in a thematic review unearths this.

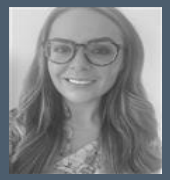
Does the business have a technical understanding of the models it uses?

- Some models built in-house may be produced by one talented individual, perhaps a specialist contractor. In their absence, this can create a knowledge gap if the user guidance and model documentation is not clearly articulated and kept up to date to maintain continuity for operating the firm's models and lead on to impacting operational resilience if those models support an Important Business Service.
- Models bought from vendors does not mean the assurance is outsourced. Where model vendors also provide validation services, it is expected that firms have a technical understanding of the model and can self-validate. The PRA expects the firm to take accountability of all its models, whether internally developed or externally sourced. Any risks borne from the models remain the responsibility of the firm.

07

DIVERSITY AND INCLUSION (D&I) IN FINANCIAL SERVICES

SASHA MOLODTSOV
Director



JENNIFER CAFFERKY
Senior Manager

D&I IN FINANCIAL SERVICES

Since the killing of George Floyd in 2020, the global pandemic, Russia's war in Ukraine, the cost-of-living crisis, climate change (and everything in between), social agendas have dominated corporate conversations, keeping Audit and Risk Committees busy. According to Harvard Business Review, "fairness and equity will be the defining issues for organisations" and as pressure for accountability and transparency grows, coupled with increased supervision by Financial Services' Regulators (PRA and FCA), diversity and inclusion (D&I) has become a fundamental risk facing Financial Services firms. And as a result, Internal Audit teams have been called to arms – a point we covered in detail within our December 2022 pack.

In February 2023, the Chartered Institute of Internal Auditors (CIIA) published its updated technical guidance on Auditing Diversity and Inclusion, clearly articulating the important role Internal Audit teams play in advancing D&I in their organisations. More too, in its recent 2023 Risk in Focus report, which surveyed 834 Chief Audit Executives across Europe, the business case for D&I mounts, the CIIA reporting citing "human capital, diversity, and talent management" as the second highest risk ranked by Internal Audit leaders (after Cyber risk).

As a more common feature on 2023/24 Internal Audit plans, we are seeing D&I typically feature alongside broader culture, talent and ESG audits or increasingly, as standalone reviews driven helping Boards and Executives assess the design and effectiveness over governance arrangements, risk management over their D&I programmes and appropriateness of their D&I plans, in context of the Regulatory expectations.

The first is the FCA's Policy Statement (PS22/3), which marked the first requirement for in-scope firms (which are primarily UK listed firms) to formally report on D&I data within their annual financial reports. More too, in-scope firms are required to disclose in annual reports from financial years starting on 1 April 2022 if they meet the following benchmarks, on a comply or explain basis:

- At least 40% of the board are women.
- At least one of the senior board positions (Chair, Chief Executive Officer ("CEO"), Senior Independent Director ("SID") or Chief Financial Officer ("CFO")) is a woman.
- At least one member of the board is from a minority ethnic background (which is defined by reference to categories recommended by the Office for National Statistics ("ONS")) excluding those listed, by the ONS, as coming from a White ethnic background).

The Regulators have given clear signals that the focus on D&I isn't going away. In January 2023, the PRA published a 'Dear CEO' letter to deposit takers in the UK setting out its priorities for 2023, which amongst financial resilience, risk management and governance, included D&I. The PRA also noted the intended follow-up to the joint discussion paper (DP 2/21 'Diversity and inclusion in the financial sector – working together to drive change' published in July 2021) which will be a Consultation Paper setting out proposals to introduce a new regulatory framework on D&I in the financial sector. On 28 February 2023, the latest Regulatory Initiatives Grid further supported this, framed as a cross-sector ESG priority, showing next steps for Diversity and Inclusion in FS, with an imminent consultation paper expected, followed by a Policy Statement towards the end of 2023.

In anticipation of this new D&I policy development, in March 2023, UK Finance members participated in a roundtable discussion, exploring possible implications of future Regulatory developments. The session explored concepts such as individual accountability, fitness and proprietary, Senior Managers' collective suitability, remuneration, representation on Boards, succession planning, risks and controls, D&I policies, setting targets, data collection and disclosure. Once the FCA/PRA Consultation Paper is published, UK Finance intends to prepare a response on behalf of members, based on this discussion and a further series of UK Finance workshops with members and the regulators.

D&I IN FINANCIAL SERVICES

Fair to say, things are swiftly moving, and it's not just in the UK. In May 2023, within the European banking community, regulatory pressure is mounting on improving diversity and inclusion too, with European Central Bank (ECB) in a recent blog 'Diversity at the top makes banks better', stating that the lack of diversity in banks was 'just not good enough'. The blog re-confirms the ECB's intention and commitment to supervise, as a priority, diversity in "an effort to boost the speed at which improvements are being made" within the banking community.

At BDO, we continue to support our clients and financial services communities on their D&I journey. A practical way BDO has been supporting Internal Audit teams explore D&I risks with senior management is by running D&I short briefing sessions and half day workshops. We are also supporting Compliance and Internal Audit teams conduct and/or support D&I reviews (on an outsourced or co-sourced basis). Typical scope areas include governance, oversight and sponsorship arrangements of D&I strategy and plans, maturity and appropriateness of D&I plans, employee lifecycle from a D&I perspective, data disclosure and targets, reporting and MI.

We have also been working with Boards; providing D&I training on some of the newer diversity considerations and the link between D&I strategy and broader ESG materiality and risk assessments.

In April 2023, at an event for FS Non-Executive Directors, BDO explored three key diversity hot topics with the following industry trailblazers:

- Sophie Hulm, CEO of Progress Together, discussing social economic diversity across the financial services sector.
- Anna Lane, CEO of Women in Banking and Finance (WIBF), sharing WIBF and LSE's latest thought leadership 'Good Finance Framework' focused on retention and attraction of women in mid-senior leadership.
- Professor Charlotte Valeur, Founder of Board Apprentice, sharing practical solutions to increasing diversity on FS Boards.

There were a number of key themes, challenges and ideas discussed, including the following:

- The Financial Services industry has the highest class pay gap of all industries.
- D&I is not about changing people – it's about optimising processes (although changing of mindsets can also be required).
- The Chair of the Board is key to ensure D&I is on the Board agenda and holding Executives to account to ensure that progress continues to be made.
- Data collection should not only be quantitative. It is vital firms understand lived experiences of individuals and take these into account (which includes consideration of intersectionality and nuanced challenges).
- There is no ambition gap – just is an opportunity gap.

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

From the perspective of the senior management team, it should not simply be about increasing representation and setting the diversity targets that Internal Audit teams will assess (although that is definitely a part of it). Regulators firmly believe that diversity of thought, driven by diversity of characteristics, experiences and backgrounds and inclusive healthy cultures, will drive market performance, promote competition, and protect consumers.

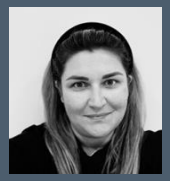
In December 2022, the FCA gave clear signals (Understanding approaches to D&I in financial services) that the financial services industry has work to do when it comes to diversity and inclusion. With this in mind, Internal Audit teams should consider the following key findings from the regulator's review to drive the planning of D&I assurance work:

- Most firms had not recognised D&I as a fundamental culture issue;
- Gender and ethnicity are receiving the primary focus and, for some firms, gender alone;
- In many cases, diversity is still being considered at a senior level and primarily for recruitment purposes, with a lack of focus for internal progression and career development paths;
- Many firms had an overreliance on D&I training, as opposed to other meaningful actions and D&I is often still seen as a Compliance 'tick-box' exercise;
- Some firms appeared publicly committed to D&I; however, strategy, embeddedness at all levels and adequate monitoring of success measures were found to be lacking.

For more information on how BDO can support your firm on its D&I journey, please speak to Sasha Molodtsov and Jennifer Cafferky.

08

ECONOMIC CRIME UPDATE



KAREN MONKS
Senior Manager

ECONOMIC CRIME UPDATE

WHISTLEBLOWING - FCA SETS OUT STEPS TO IMPROVE WHISTLEBLOWER CONFIDENCE

The FCA has recently published its commitment to improve the confidence of whistleblowers. The FCA recognises the importance whistleblowing disclosures play in providing the FCA with unique insights into the firms and markets that it regulates. Between April 2021 and March 2022, the FCA received 1,041 whistleblowing disclosures, which led to:

- significant action to manage harm in three cases which may include enforcement action, a Skilled Person review, or restricting a firm's or individual's permissions;
- action to reduce harm in 96 cases which may include writing to or visiting a firm, asking it for more information, or asking it to attest to complying rules; and
- 99 cases informing the FCA's work including harm prevention, but with no direct action.

In January 2022, the FCA contacted firms who had engaged with the Whistleblowing team to take part in a qualitative assessment survey to understand how whistleblowers had found their interactions with the Whistleblowing team. Of the 68 participants invited, 21 completed the survey. The survey consisted of 25 questions, which focused on the FCA's key contact points, and, overall, the results have provided some key insights on how the FCA's whistleblowing arrangements have been perceived. Of the 21 respondents:

- 13 answered that the reason for reporting to the FCA was because the respondent had made an internal compliant that was ignored;
- 12 were dissatisfied with the FCA Whistleblowing team in relation to listening;
- 15 were dissatisfied with the FCA Whistleblowing team in relation to exploring the issues reported. In particular, a number of the respondents did not feel that there had been enough dialogue with them to ensure that their concerns had been understood.
- 15 were dissatisfied with the FCA's handling of their whistleblowing report.
- As part of the reporting process to the FCA, a respondent can choose to be kept informed of the outcome of the review of the disclosure by the Whistleblowing team. 17 of the respondents surveyed elected to be kept informed, of which 10 answered that they did not find the Whistleblowing team's progress updates to be sufficiently reassuring. Respondents felt that the updates provided 'lacked substance', 'no real information was given' and 'didn't say if the FCA was investigating or not'.
- 8 of the 9 respondents who had received final feedback were dissatisfied with the outcome that they had received. Some respondents said that they did not understand how the FCA had used their information. Some respondents felt that their concerns had been 'brushed aside', and some felt that there were 'no real consequences' for wrongdoers.

ECONOMIC CRIME UPDATE

Overall, the FCA have said that they are disappointed with the level of dissatisfaction expressed by many of the respondents. The FCA will look to improve the feedback provided to whistleblowers when they are provided with conclusive communications. Feedback from the regulator will also include the measures taken, the rationale for those measures, as well as the reasons behind no action being taken on the basis of the whistleblowing report to ensure the outcome is as clear as possible.

What should internal audit teams think about?

Whistleblowing disclosures from firms remain an important regulatory tool for the FCA and we expect there to be continued focus on the systems and controls firms have in place to enable employees to make an internal disclosure through a firm's Whistleblowing process, as well as the FCA.

SYSC 18.3.1 requires firms to establish, implement and maintain appropriate and effective arrangements for the disclosure of reportable concerns by whistleblowers.

With this in mind, Internal Audit teams should evaluate the firm's Whistleblowing framework to ensure that arrangements :

- are capable of handling disclosures where the whistleblower has requested confidentiality or has chosen not to reveal their identity.
- allow for disclosures to be made through a range of communication methods.
- support the effective assessment and escalation concerns, where appropriate, including to the FCA or PRA.
- Include a mechanism to provide feedback to a whistleblower, where this is feasible and appropriate.

When planning assurance work for the firm's management of Conduct Risk, it is recommended that IA teams consider including a review of the whistleblowing arrangements to ensure that there is a clearly documented framework in place and all employees are aware of the process, should they have a concern.

UK FRAUD STRATEGY

On 3 May 2023, the UK government published its long-awaited Fraud Strategy, with the aim of reducing fraud and cybercrime by 10% by 2025. Delivery of this strategy is to be phased over a 3-year programme of work to the end of 2025, which will be led and governed by the Home Office.

The key measures to be introduced include:

- establishing a new National Fraud Squad with over 400 new posts and making fraud a priority for the police through the Strategic Policing Requirement.
- deploying the UK intelligence community and leading a new global partnership to pursue fraudsters, wherever they are in the world.
- replacing Action Fraud with a new state of the art system for victims to report fraud and cybercrime.
- banning cold calls on all financial products so fraudsters cannot dupe people into buying fake investments.
- enabling payment service providers to adopt a new risk-based approach to provide additional time for potentially fraudulent payments to be investigated.
- legislating to enable the Payment Systems Regulator ("PSR") to require reimbursement of all authorised fraud victims by all PSR-regulated payment service providers.
- requiring the FCA to undertake assessments of the fraud systems and controls within financial services firms.
- working with industry to make sure that intelligence is shared quickly with law enforcement.
- overhauling and streamlining fraud communications so that people know how to protect themselves from fraud and how to report it.
- making the tech sector put in place extra protections for its customers, via the Online Safety Bill and an Online Fraud Charter and introducing tough penalties for those firms that do not.

What should internal audit teams think about?

Assurance over fraud risk management needs the internal audit team to ensure:

- that the business-wide risk assessment sufficiently considers the fraud risks associated with the business model.
- a review of the fraud risk controls is on the plan and that the assessment is in line with the exposure fraud risks. Where any weaknesses are identified, a remediation plan should be put in place to address these.
- there is a clear message and top-level commitment from the senior management regarding the firm's fraud prevention agenda.
- there is a robust Fraud Response Plan in place and that it is periodically assessed in order to ensure that it remains up-to-date and appropriate.
- that annual training plans include fraud awareness/prevention training which incorporate the latest known regulatory guidance and industry good practice.

FOR MORE INFORMATION:

RICHARD WEIGHELL
Partner

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

www.bdo.co.uk

42020160