INTERNAL AUDIT SUPPORT

BANKING & BUILDING SOCIETIES

May 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 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

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 may 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

LUKE PATTERSON
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 Luke Patterson.

1. What has been your career leading into BDO?

I have had a varied career to date, starting in a small three office firm in Uxbridge creating management accounts and undertaking external audits. I chose to do ACA even though my firm did not want me to. I stuck to my guns, and they eventually relented – I succeeded in getting my letters in 2004. I eventually outgrew them and moved around a bit until I landed at a top 10 firm in Luton where I was introduced to Financial Services (London) performing Internal Audit, External Audit and Public Sector work. I really enjoyed my time there as the diversity of jobs was interesting. Externally auditing large Government departments was interesting and eye-opening.

I eventually decided that Financial Services was where I wanted to go for the complexity of projects and great people that work in the sector. I then moved on to a Big Four firm, before quickly realising that a Big Four firm was too restrictive, especially since I was an experienced hire by then. I then went in-house for a well-known insurance firm and realised that I quickly became bored by the relatively slow pace of industry and joined BDO Financial Services Advisory in 2015 as a very experienced Senior Manager and have never looked back!

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

My role in Financial Services Advisory is varied. I lead:

- A portfolio of Internal Audit engagements, supporting my clients in either outsourced or co-sourced internal audit within the Insurance, (GI / Life), Payments and Pension sectors.
- BDO's Safeguarding offering to the market for Payments Services and Electronic Money firms.
- Engagements under SOX regulatory compliance (US listed rules) for controls and process reviews.
- FS Advisory's internal Quality and Risk processes by acting as a sounding board for client take-on, due diligence, etc.
- Data Analytics interactions between FS Advisory and other parts of BDO to help embed data analytics in our professional practice.
- Involvement in external industry groups, such as ICAEW Safeguarding committee and ICAEW Crypto Regulatory committee.

What I really like doing is supporting other people, either our BDO team or our clients to help them overcome issues, problems or to "grease the wheels" to allow them to do their job easier.

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

I undertake a number of regulatory and required work engagements for a few high street branded, very well-known financial services US listed clients, but the most interesting element of my job currently is the wider consultation that the UK regulators and HMRC are having on Crypto within the UK FS market. I lead the ICAEW regulatory response to the HMRC's consultation on Crypto Regulation. Working with all significant accountancy firms in the UK and University professors to respond to the wider need for Crypto regulation was really interesting, to be on the cutting edge of regulation and being able to feed into the process.

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

The Internal Audit team have a huge and varied skill set and come from all parts of the business, countries and life. There is no one perfect model internal auditor. As a result, the team is highly diverse in several ways that makes life colourful and interesting to be around and work with. The team is continuingly growing and developing and bringing new ideas to the table. The team (at all levels, including partners) are happy to interact and listen to anyone who has a good idea.

5. What drives you to do what you do?

I mentioned earlier that I get out of bed to help people, either my team or my clients. This allows me to get involved in a variety of things and variety is what I enjoy. No one day is the same.

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

The varied nature of my journey to date and the ability to switch and pivot to my preferred sector, type of work has surprised me as to how easily it was to do and accepted, especially by BDO. This has not changed as my career continues to progress.

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

Be curious. If you like to understand how things work, feed the curiosity.

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

Key areas that I am talking about with our own team and clients include the use of Data Analytics, Artificial Intelligence and ChatGPT. All I know is that if we are doing the same thing as we are doing now in 5 years' time, we will be almost irrelevant to meet our clients' needs. The firms that succeed will be the ones that embrace the best of the changes coming down the line.

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

Basketball has been a lifelong love of mine both playing, socialising and recently coaching my Under-12 and Under-14 local teams. I have had the pleasure of playing for the top league in the UK and attending US scouting camps and the experiences I have gained was invaluable.

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

Good book, sunscreen and a 65-foot fully equipped and staffed super yacht!

03

ESG UPDATE

HOW EFFECTIVELY IS YOUR FIRM IMPLEMENTING ITS CLIMATE CHANGE RISK MANAGEMENT AND REPORTING FRAMEWORKS?

ADAM SOILLEUX
Associate Director

GLORIA PEREZ TORRES
Senior Manager

IMPLEMENTING CLIMATE CHANGE RISK MANAGEMENT AND REPORTING FRAMEWORKS

What should Internal Audit teams consider for control testing?

Latest developments

Regulators and the Government have been busy publishing environmental, social and governance ("ESG") updates over the last few weeks:

- 30 March: HM Government published its update to the 2019 Green Strategy
- 5 April: FCA published its 2023/ 2024 Business Plan
- 18 April: PRA's Executive Director, Financial Stability Strategy and Risk, published a speech on the financial sector progress on climate action which was given at Chapter Zero's fourth anniversary dinner

These publications remind regulated firms of their obligations to manage climate change financial risk and report on their progress in alignment with the Task Force on Climate-Related Financial Disclosures ("TCFD") framework.

Speech by Sarah Breeden, Executive Director, Financial Stability Strategy and Risk: 'Climate action: approaching a tipping point?'

Breeden manifested that she had hoped to have seen stronger linkages between climate change and strategic decision-making process across the economy. This means that regulated financial institutions have not sufficiently considered their climate-related financial risks and opportunities arising from the transition to a lower carbon economy such that findings are used in strategic decision-making processes. In discussing the challenges to advancing the transition, building capability was listed as first, followed by unexpected political and economic turmoil, lack of clarity on the Government's policy and difficulties with system-wide change.

On TCFD reporting, it was announced that the Bank of England is soon to publish its fourth TCFD-aligned report which will provide firms with an example of what good looks like.

Finally, Breeden reminded firms of the expectations set out in the PRA's latest Dear CEO letter and the Supervisory Statement (SS3/19) and indicated that the PRA will be looking at how firms are meeting those expectations in practice. Firms should, therefore, consider the extent to which they have embedded their frameworks and also when and how they are considering climate change risk in decision making, as well as how this is being documented and monitored.

FCA's ESG Strategy

The FCA's 2023/ 2024 Business Plan sets out how it will deliver the second year of its three-year strategy. It reflects the FCA's belief that sustainability-related matters continue to become increasingly material for the sector's future prospects and, therefore, the regulator's plan is to monitor how effectively firms are implementing climate-related financial disclosures. This will be undertaken through direct supervision and implementing the FCA's Strategy for Positive Change, which is focused on the following ESG priorities:

- Strengthening the quality of sustainability-related disclosures through assessing how the final International Sustainability Standards Board's ("ISSB") standards (expected to be released in June 2023) will be implemented in the UK;
- Providing a Feedback Statement to the Discussion Paper on ESG governance, incentives, and competence; and

IMPLEMENTING CLIMATE CHANGE RISK MANAGEMENT AND REPORTING FRAMEWORKS

What should Internal Audit teams consider for control testing?

- Finalising and publishing the rules on Sustainability Disclosure Requirements and investment labels, and beginning the implementation process potentially in Q4 2023 to strengthen consumer protection and trust in the markets for ESG-related investment products.

UK Government publishes updated Green Finance Strategy: Key takeaways for UK firms

The UK Government's much-anticipated updated Green Finance Strategy is an update of the 2019 Green Finance Strategy which seeks to ensure the UK becomes a world leader on green finance and investment. There is a clear focus on ensuring that the sustainability and climate change legal framework is further developed. We also observed a focus on ensuring that more tools are developed to help firms with advancing their transition plans to a lower carbon economy. Some of the key developments that we expect will impact ESG-related reporting and disclosure obligations for UK companies over the next 12 to 24 months include:

- A consultation on the implementation of a requirement to disclose decarbonisation plans for larger UK companies. This is building on the current requirement for listed companies, as well as large asset owners and managers to disclose transition plans on a 'comply or explain' basis;
- The development of a framework to assess ISSB IFRS Sustainability Disclosure Standards for their suitability for adoption in the UK as soon as these are published (expected summer 2023);
- Launching a call for evidence on Scope 3 greenhouse gas ("GHG") emissions reporting, aimed at improving the understanding of the costs and benefits for producing and using this information and updating the Environmental Reporting Guidelines, including for Streamlined Energy and Carbon Reporting which provides voluntary guidance for UK firms on how to measure and report emissions;
- The delivery of the UK's Green Taxonomy in Autumn 2023 to provide investors with definitions of which economic activities should be labelled as green; and
- Regulating ESG ratings providers to ensure better outcomes for these products.

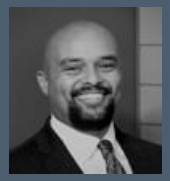
Firms should monitor developments in the aforementioned areas within Q3 and Q4 2023 and these should be considered when carrying out internal audit work to ensure the business is meeting all relevant regulatory requirements and expectations.

04

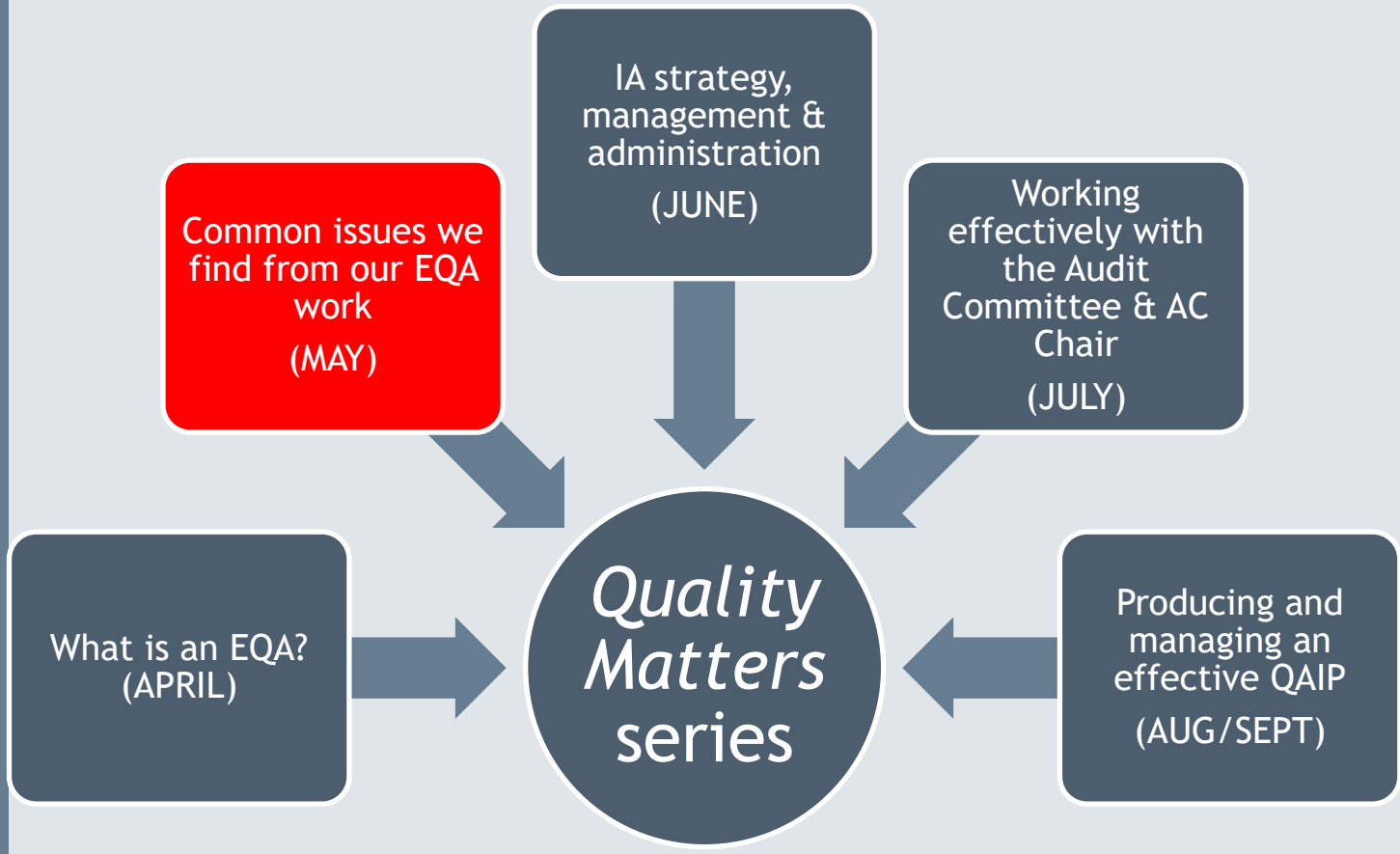
QUALITY MATTERS
PART 2

COMMON ISSUES WE FIND FROM OUR EQA WORK

SAM PATEL
Partner



BRUK WOLDEGABREIL
Associate Director



QUALITY MATTERS – PART 2

Common issues we find from our EQA work

In our April pack, we explored the concept of an External Quality Assessment (EQA) at a high-level and the good practices that an Internal Audit (IA) team and a Head of Internal Audit (HoIA) should consider before, during, and after an EQA process to maximise the assessment's outputs.

This month, we delve deeper into the common challenges and issues we've observed from our EQA engagements.

Typically, firms are generally good at meeting the basics of the requirements set out in the global IIA standards, Code of Ethics and CIIA Internal Audit Financial Services Code ("FS Code").

Having performed a number of EQAs over the last few years, from one-man bands to teams with over 500 auditors, we as an advisory team have gathered some key common findings related to the guidance teams should follow, as well as our insights on matters arising from a general IA perspective and not linked to a specific aspect of the guidance or standards.

AUDIT PLANNING

The basis of an audit plan needs to be a comprehensive audit universe, which itself is built upon several inputs including (non-exhaustively) the firm's:

- strategic plan;
- risk management framework outputs (e.g., firm-wide risk assessments, risk register);
- key business functions (and their individual Risk and Control Self-Assessments);
- regulatory and legal requirements; and
- FS Code considerations.

We sometimes find that an IA team produces an audit universe, but many of the audit areas within the universe have not been reviewed for a period of time. This could be a material issue if the full set of auditable areas for a firm has not kept pace with regulatory developments, business changes or sufficiently adapt to the firm's current strategic plan. Such a scenario would leave the firm with blind spots on key risk areas and vulnerable to significant risk impacts, e.g., insufficient audit coverage of operational resilience controls proceeded by a systemic failure of the firm's payment systems for more than a tolerable period (customer impact, financial impact, regulatory impact – the list goes on). Keep in mind PS 2010.A1 ("Planning") – there should be an annual, documented, re-assessment of risks and feedback from the senior management incorporated into the planning process.

As a corollary point, where we find an obsolete audit universe, invariably we have also noted instances of the Audit Committee (AC) Chair unaware that important risk areas have not been reviewed by the IA team or have been removed from the annual plan by the HoIA without sound (documented) rationale. This effectively means that the AC is unable to decide based on the full picture and, therefore, hampered in its role to constructively challenge the Executive on addressing key risks. Again, consider PS 2010.A2 ("Planning") – the plan must consider the Board and AC's expectations and an EQA will flush this out when a request is made for evidence of the HoIA opening up their planning process to gather Board views.

Insufficient audit planning also generally gets picked up in assessing review types during an EQA process:

- **Lack of thematic reviews**: if the audit universe is insufficient on capturing the key risks, there's no reasonable expectation that it will consider specific cross-cutting themes, e.g., culture, that will broadly permeate every auditable area of the firm and should be addressed through a firm-wide thematic review.
- **Lack of end-to-end reviews**: a follow-on to thematic reviews, audit planning should also consider end-to-end reviews of specific processes that straddle multiple functions in the firm. A good example is management information reporting to the Board; a regularised process of gathering information on key metrics across the firm, to be standardised, checked, challenged and reported on a timely basis requires numerous controls that can often be overlooked as they sit in between functional audits.

QUALITY MATTERS – PART 2

Common issues we find from our EQA work

- **Cyclical reviews**

- Omitting regular review areas that would be expected by the FCA, PRA or, at a minimum, expected in the FS Code but missing from the audit plan without justification, e.g., liquidity, capital, corporate governance. The Regulator would likely pick up on this when firm documents are requested as part of supervisory engagements.
- Certain auditable areas may have once received regular review but have since become deprioritised over the course of years owing to other significant issues requiring urgent attention. Without sufficient documentation underpinning the planning process to help track what should still be cyclically reviewed as a recurring key risk to the firm, topical issues prioritised today may inadvertently steer the firm to face impact from risks sitting right under the firm's nose.

- **Reviews led by available skillsets, not key risks**: we've previously explored, in our March pack, the challenges involved in Resource Management. A common consequence from resource limitations, and a lack of skilled co-source support, is an ineffective audit plan built upon auditable areas that can only be addressed by the skillset available in the IA team, and not on the key risks faced by the firm. This is generally borne out in EQA interviews with IA team members when queried about the IA planning process. Heads of Internal Audit should keep in mind PS 2020 ("Communication and Approval") to evidence that they have communicated the impact of resource limitations for delivery of the audit plan to the AC to escalate the issue and thereby access further options (budget) to deliver the key parts of the plan with external support.

ENGAGEMENT PLANNING AND EFFECTIVE RESOURCE MANAGEMENT

Considering planning issues at the engagement level, EQAs can often unearth instances where the technical skills and level of resources required to provide sufficient assurance over a complex subject or business area have been underestimated.

A common example is a Cyber review, which may be budgeted for 10 days by the HoIA, but, given the scale and depth of information systems for a typical firm, could reasonably be budgeted between 30 – 40 days, perhaps more if internationally co-ordinated with other sites. The 10-day review will have taken place, and a report made to the AC that Cyber has been covered in the audit plan; but the AC will not have appropriate context to understand the breadth of scope behind the review, especially scope exclusions, and the limited amount of testing that would have been permitted within a such a short review period.

DOCUMENTING EVIDENCE AND WORKPAPERS / DEMONSTRATING ENGAGEMENT SUPERVISION

EQAs examine the documentation behind a sample of reviews to assess if the IA activity policies and procedures have been followed. There are several common issues that crop up from our routine documentation review, including:

- **Explicitly confirming scope exclusions in the engagement scope**: scope exclusions help to define a clear perimeter on what the review is seeking to cover so that the audit team can effectively focus its finite time and resources for maximum coverage and the report user can be confident that the key risk areas have received the full attention of the engagement team. To provide positive assurance – the highest form of assurance – without clear scope exclusions opens the audit report up to innumerable criticisms from its stakeholders as to whether risks were addressed and if resources were effectively managed.

QUALITY MATTERS – PART 2

Common issues we find from our EQA work

- **Evidence of scope and final report reviews by HoIA**: engagement supervision is critical to safeguarding quality in the team's auditing work (PS 2340 – "Engagement Supervision") and, from our market experience, a highly effective method to develop the IA team's skillset. Where we find that there is a lack of supervision at key milestones around planning and reporting stages, we also generally find issues in the quality of the audit work and credibility of report conclusions.
- **Finding the "Golden Thread"**: analogous to Charles Dickens' second novel in the three-part "A Tale of Two Cities", the Golden Thread within internal audit is the work programme, which stitches the engagement plan, testing and final report, by bringing together the risks to be addressed, controls assessed and testing outcomes together with the supervisory oversight evidenced (both before and after testing). If the golden thread is found to be missing, our assessment of the IA team's audit practice would have to deepen to gather more reviews for assessment and evaluate if the issue is systemic to the work of the whole function.
- **Changes to draft reports not being reflected in working papers**: workpapers are the substance of the IA's assurance work and, therefore, need to reflect the input of engagement supervision and any external co-source SME views factored into the reporting so that amendments to the findings, observations and recommendations can be justified, if challenged by the AC, and scrutinised if subsequently found to be faulty (e.g., skilled person review uncovers that findings in an audit report were redacted before being published to the AC which would otherwise have helped flag a key non-compliance issue to the Board ahead of a risk impact).
- **Documenting any deviations from methodology**: while it is the duty of the HoIA to establish policies and procedures (PS 2040 – "Policies and Procedures"), it is the responsibility of IA team members to identify where engagement procedures have had to deviate from the approved IA methodology to effectively arrive at conclusions. In EQAs where we assess problematic reviews, e.g. findings that have been sternly challenged by the auditee, the IA team may have either inadvertently deviated (lack of training or induction process) or intentionally deviated and not informed the audit manager (lack of engagement supervision, poor team co-ordination or morale). In most circumstances, it's driven by the audit engagement team insufficiently justifying the sampling approach and sampling sizes that could lead to wide variations in testing outcomes and, ultimately, the final report to the business under review. One of the key benefits from documenting a sampling approach, aside from evidencing methodology, is that it can address most data and technical challenges raised by the auditee and offer the opportunity to re-sample and re-test controls efficiently.

FOLLOW UP / OPEN AND OVERDUE ACTIONS

Most IA teams we assess in our EQAs are generally very proactive at following up on open issues and putting resources in place to close these down on a timely basis. However, where there are issues in closing actions, we often see severely overdue actions – but this is typically a symptom of one or multiple factors, such as:

- **New due dates**: we have seen open actions being given a new due date multiple times, such that the AC has lost sight of when the issue and associated action was initially raised by the HoIA. In assessing IA and Board materials within an EQA, we have tracked the same 'high priority' open actions from AC pack to AC pack that extend over several years. Large-scale transformation or change projects are generally the root cause of never-ending open issues, a hot topic we covered in greater detail in our September 2022 pack.
- **Tactical vs. Strategic solutions**: often the big issues that remain open are chasing a big, strategic, solution to arrive that may well take years to land. A pragmatic approach for addressing a large open action could be to focus on short-term tactical fixes in advance of a strategic solution. A common example would be User Access controls testing – as most "preventative" solutions for partially effective controls are strategic in nature (e.g., brand new security platform to manage user access), the issue could be addressed in the near term by a "detective" solution (e.g., scheduled check on accesses used on a periodic basis) to identify and address breaches. The alternative would be a risk and open action dropping back into the 'wallpaper' of regular action reporting, opening the firm up to vulnerabilities from risks yet to be addressed in legacy reviews.
- **Culture in the firm**: aside from due dates and scale of solutions, we have also found that limited challenge provided by the AC, at least by what is evidenced in the meeting minutes, could be a key driver for inefficient progress on open actions. This itself could be an indicator of wider culture issues in the firm where 'tough conversations' on key risks may be avoided due to boardroom politics or deference to income generators in the business.

We look forward to sharing the next instalment of our "Quality Matters" series in June where we explore IA strategy, management and administration insights gathered from our EQA and quality assurance work.

05

WHAT INTERNAL AUDIT MODEL WILL BEST SUIT YOUR NEEDS?

MICHAEL HADDON
Principal

WHAT INTERNAL AUDIT MODEL WILL BEST SUIT YOUR NEEDS?

For many small to medium sized firms, the question often arises as to which is the best operating model for its internal audit function – outsourced, co-sourced or predominately in-house?

First off, for most, if not all small to medium sized firms, establishing a predominately in-house function is just too costly when considering the wide variety of skills and types of technical knowledge required to deliver all the reviews of a typical annual plan – something we have explored in March's pack. That leaves the outsourced and co-sourced options and as to which is the right model, the simple answer is: it depends.

Each model understandably has its benefits and costs, its pros and cons, and the relative weighting of these will be specific to a firm's current and future circumstances, business profile and strategy.

The key factors that determine which model is likely to provide the most effective internal audit function now, and into the foreseeable future, can include:

- Is the firm at an early stage of development?
- Does the firm have significant growth plans (organic and/or through acquisition)?
- Is the firm entering a period of relative stability and modest growth?
- Does the firm have an established operating model and culture which aligns to either IA model?
- Has the firm experienced good or poor outcomes from either IA model?

In addition, consideration of some key criteria helps with the decision, in particular is the firm primarily looking to improve efficiency, to enhance technical quality, or to reduce or better control costs?

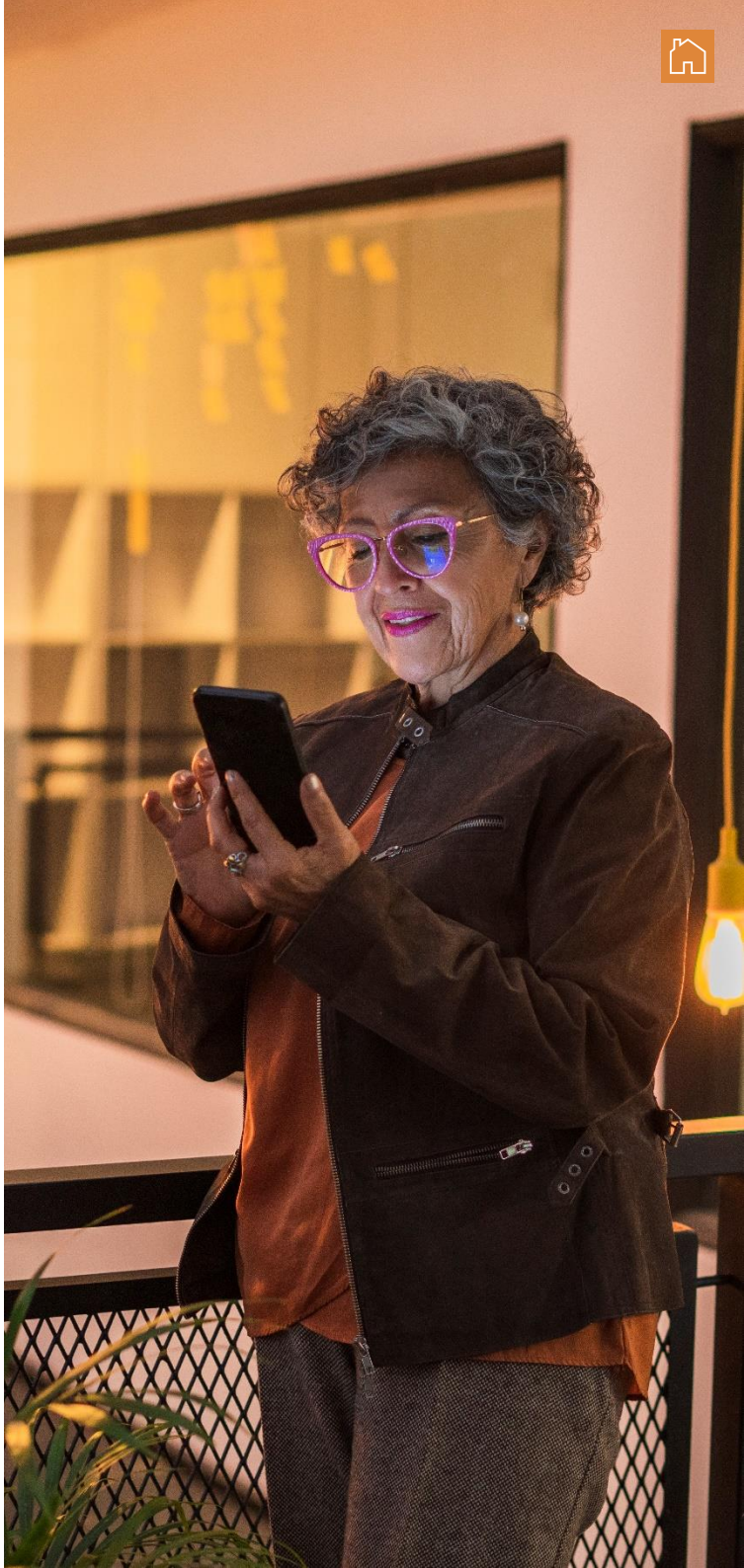
In broad terms, our market experience tells us a young and evolving firm is likely to benefit from an outsourced model but as it matures, or enters a period of significant change, a co-sourced model is then likely to be more effective.

Again, not a universal prediction, rather a general trend that we tend to pick up on from our multi-year client relationships involving both assurance and advisory work.

Our experience typically suggests that in a young/evolving business, there are likely to be many priorities and pressures on a relatively small management team. In these circumstances, adopting an outsourced model provides an immediate, viable solution to the firm's third line assurance needs, and so gets an important action off the 'to do list' right away. It also provides the firm with cost-effective access to a wide range of specialists which can add a lot of value as a firm seeks to establish a compliant risk and control framework.

As a firm grows and/or goes though significant change (such as a change in business model, an integration, a change in ownership, etc.), transitioning to a co-sourced model, with an in-house Head of Internal Audit, can help to maintain effectiveness. In such situations, establishing a degree of in-house capacity helps internal audit to connect with a wider set of stakeholders, to get things done more quickly and to make changes 'stick' more effectively relative to an outsourced provider. It also has the added benefit of being closer to the business which means it can more quickly identify and contextualise issues and emerging risks given its day-to-day presence.

While transitioning to a co-sourced model is likely to maintain effectiveness in these circumstances (by being relevant, staying on track and closing issues with less boardroom pain), in our view, it is not likely to enhance technical quality, nor is it likely to reduce cost (although it may be cost neutral).



WHAT INTERNAL AUDIT MODEL WILL BEST SUIT YOUR NEEDS?

WHAT SHOULD INTERNAL AUDIT TEAMS THINK ABOUT?

As a firm matures (and achieves a robust control environment) and activity levels become more stable, strengthening the in-house team is also likely to be a more effective approach for the longer-term. In this situation, a greater proportion of the annual plan can be delivered by the in-house team, with the co-sourced partner supporting with subject matter expertise and/or limiting its role for full reviews to the more technically complex areas such as cyber security, prudential risk, etc.

For Heads of Internal Audit, transitioning to a successful co-sourced model should not present any significant challenges assuming the following are in place:

- Appointing the right calibre and personality of individual(s) to the in-house role(s) such that sufficient technical coverage can be realised from the investment
- Clarity of role and expectations between the in-house team and co-sourced partner, for example finalising of internal audit deliverables and getting these across to management and collating management responses
- Clarity on the level of support that will be needed on individual reviews and the expectations on who will present internal audit reports at the governance forums such as the Executive Risk Committee and the Audit Committee

For a sustainable co-sourced model, it is also important for Heads of Internal Audit to monitor performance and guard against the following:

- Auditing to capacity and capability (best efforts) rather than what the areas need from a technical/coverage perspective
- Falling behind on good practices, hot topics, regulatory developments, etc.
- Failing to recruit and retain a high-quality team
- Getting too close to the business
- Inability to provide a fresh perspective and objectivity over time.

06

ECONOMIC CRIME UPDATE

CLARINDA GRUNDY
Associate Director

ECONOMIC CRIME UPDATE

New UK 'failure to prevent fraud' offence finalised

In our February pack, we discussed the UK Government's intention to implement a 'failure to prevent fraud' offence. This has since crystallised, and there have been a number of additional developments in the financial crime space over the last several weeks. Notably, the FCA's 2023/24 Business Plan which highlights a continued focus on financial crime, including fraud, encouraging Banks and Building Societies to continue to promote the topic as a top agenda item.

On 11 April, the UK Government finalised the new UK 'failure to prevent fraud' offence, aiming to prevent and deter fraud by making it easier to prosecute a firm if an employee commits fraud for the firm's benefit. Larger firms may face up to an unlimited fine if found guilty, whereas small and medium sized enterprises are exempt.

The offence will be included in the Economic Crime and Corporate Transparency Bill. Regulations are already in place for failure to prevent bribery and the facilitation of tax evasion which have been considered poignant in preventing and deterring their respective criminal activities, and thus it is expected that this new legislation will have the same impact and effect.

The offence applies to all sectors. However, to ensure burdens on business are proportionate, only 'large' organisations are in scope – defined (using the standard Companies Act 2006 definition) as organisations meeting two out of three of the following criteria: more than 250 employees, more than £36 million turnover and more than £18 million in total assets. This definition applies to businesses, not-for-profit organisations (such as charities) as well as incorporated public bodies.

Organisations will be able to avoid prosecution if they have reasonable procedures in place to prevent fraud.

The offence will be in force once the Economic Crime and Corporate Transparency Bill has received royal ascent (and becomes an Act) and guidance on reasonable prevention measures has been published by the UK Government.

What should Internal Audit teams think about?

Importantly, while small and medium sized enterprises will be exempt from the new offence, firms which fall into these classifications should still treat fraud prevention as a priority and take note of the new offence and incoming guidance as a matter of best practice.

Whilst Government guidance on reasonable prevention procedures has not yet been published, larger firms in scope for the new offence should be proactive in ensuring their frameworks are adequate. The 'reasonable procedures' defence mirrors that found in relation to tax evasion in the Criminal Finances Act 2017, therefore large organisations should broadly be prepared for Government guidance to focus on the following elements:

- **Top-level commitment** – firms should ensure that there is clear involvement from senior management especially in any key decision making for counter fraud frameworks. There should be a clear 'tone from the top' with respect to fraud prevention across an organisation.
- **Risk Assessment** – firm's should undertake a business-wide fraud risk assessment in order to understand and assess their fraud risk exposure and determine the effectiveness of their mitigating controls

ECONOMIC CRIME UPDATE

- **Policies and procedures** – firms should ensure that fraud policies and procedures are proportionate and risk-based, aligning to the risk assessment.
- **Due diligence** – firms should ensure that due diligence procedures are in place for those who perform or will perform services for or on behalf of the firm.
- **Training** – firms should ensure that staff are trained on what might constitute an offence and lead to a prosecution. For example, a firm might face legal action if employees were selling products to a customer under false pretences.
- **Monitoring and review** – firms should ensure their fraud prevention procedures, systems, and controls are subject to ongoing review, with improvements made where necessary.

Economic Crime Plan 2 launched

On 30 March the UK Government published its Economic crime plan 2023 to 2026 (coined 'Economic Crime Plan 2' or 'ECP2'). ECP2 builds on ECP1 (2019-2022) to set out what the public and private sectors should do to continue to transform the UK's response to economic crime.

ECP2 places a greater emphasis on the importance of engaging the whole ecosystem when it comes to financial crime prevention, sharing knowledge, insights and intelligence across both public and private sector organisations. As well as specific outcomes-focussed priorities and plans relating to money laundering and sanctions, ECP2 additionally sets out the strategy towards fraud prevention.

Ultimately, ECP2 endeavours to ensure that the UK remains a transparent, safe and open places for firms of diverse types and sizes to do business to promote economic growth in a sustainable manner.

What should Internal Audit teams think about?

- Turning the macro into the micro, Banks and Building Societies of all sizes should read ECP2 and reflect what impacts it might have on the business both now and over the coming 3 years. ECP2 can be used as the basis for horizon scanning and road mapping potential incoming process and control changes.
- Firms should be agile and responsive and, in particular be alive to imminently incoming nation-wide initiatives (including the Government's new SAR platform, Companies House reform and sanctions regime amendments).
- Firms should also turn their focus to the information and intelligence gained through BAU activity and evaluate whether this can be enhanced to provide better quality intelligence internally, to other Banks and Building Societies, to the wider financial services sector, and to other sectors in the fight against financial crime.

For further detail on ECP2, please refer to the article we published in April.

Payments "Dear CEO" letter from the FCA

On 16 March, the FCA published a 'Dear CEO' letter setting out its priorities for Payments firms. The letter places an expectation on payments firms to deliver 3 main 'outcomes' relating to ensuring that customer money is safe, ensuring that the firm does not compromise financial system integrity and meeting customers' needs with respect to high quality products and services, competition and innovation and robust implementation of the FCA Consumer Duty.

Within the 2nd 'outcome' ('ensure that your firm does not compromise financial system integrity'), the first and second priorities set out by the FCA relate to Money Laundering & Sanctions and Fraud respectively. The FCA notes that its reviews of Payment Institutions ('PIs') and Electronic Money Institutions ('EMIs') over the preceding 24 months have highlighted a number of common issues. These include, but are not limited to:

- **Money Laundering & Sanctions** – customer due diligence and enhanced due diligence, risk assessments and screening.
- **Fraud** – lack of awareness and engagement, backlogs and control weaknesses.

ECONOMIC CRIME UPDATE

What should Internal Audit teams think about?

The Dear CEO letter is not directly aimed at banks or building societies. However, banks in particular which are the banking partner of the PIs and EMIs should pay attention to the letter. Banks offering services to PIs and EMIs may wish to use the FCA Dear CEO letter (and the recommendations which it makes) as a basis for the scope for a periodic audit/independent review on the adequacy of the firms' financial crime prevention systems and controls. Key areas of the PI and EMI frameworks for consideration per the letter include:

- **Money Laundering & Sanctions**

1. Ensuring that the AML and Sanctions business wide risk assessment is reviewed and updated regularly, and informs AML and Sanctions controls
2. Regularly assessing the AML and Sanctions compliance framework and remediating promptly if necessary
3. Identifying, investigating and (where necessary) reporting instances of suspicious or unusual activity through Suspicious Activity Reports ('SARs')

- **Fraud**

1. Ensuring that the fraud risk assessment is reviewed and updated regularly, and informs anti-fraud controls
2. Regularly assessing the fraud prevention framework to determine effectiveness, and making prioritised upgrades as necessary
3. Collecting and retaining robust customer due diligence records, both at onboarding and on an ongoing basis, to identify and prevent accounts being used to receive or transfer the proceeds of fraud (or other financial crimes)

Wolfsberg Group publishes new ABC compliance programme guidance

On 17 April the Wolfsberg Group published its updated Anti-Bribery and Corruption ('ABC') Compliance Programme Guidance. The guidance aims to support firms in embedding a risk-based approach to prevent, detect, and report acts of Bribery and Corruption.

The core components of the updated guidance include:

- Implementing a tailored and appropriate firm-wide ABC policy;
- Defining roles and responsibilities with respect to ABC compliance;

ECONOMIC CRIME UPDATE

- Undertaking risk assessments on an ongoing basis and used to drive development and maintenance of controls;
- Deploying an ABC training and awareness programme;
- Monitoring and testing to be undertaken relating to the ABC control framework on a regular basis.

Building on the ABC guidance published by the Wolfsberg Group in 2017, the updated 2023 guidance also:

- Incorporates lessons learnt from enforcement which has taken place in the interim period. In particular;

1. Red flags have been updated; and
2. Transaction corruption risks sections have been expanded;

- Emphasises the need for continual evolution and enhancement of a financial institution's ABC framework;
- Contains a new section on identifying, reporting, and mitigating emerging Bribery and Corruption risks;
- Aligns to current and evolving legal and regulatory expectations, in particular with respect to post-acquisition due diligence and holistic risk assessment.

What should Internal Audit teams think about?

This guidance is likely to be of particular importance to those in roles which oversee the ABC compliance arrangements, this may be a part of the role of the MLRO or alternatively a dedicated Head of ABC/function lead. Key considerations for third-line assurance over such roles include:

- **Top-level commitment**: Senior Management should be actively engaged in the ABC agenda, disseminating consistent and strong tone from the top and leading control framework development and approval;
- **Risk Assessment**: Firms should ensure risk assessments are holistic and undertaken on an ongoing basis to understand the evolving exposure to Bribery and Corruption risks, and used to implement proportionate and robust controls to mitigate and manage these risks. Such controls should focus on covering risks associated with anything of value, third party providers and customer related transaction risks, investments and acquisitions;
- **Policies and procedures**: Firms should have a firm wide ABC policy which is tailored to the unique business size, operating model and footprint of the firm. A firm's procedures should contain specific steps to support staff in identifying, reporting and mitigating existing as well as emerging Bribery and Corruption risks and red flags;
- **Training**: Firms should ensure that staff are trained on key Bribery and Corruption risks and controls. Case studies should be incorporated into training to share lessons learned from internal and external events to iteratively enhance the ABC compliance programme and internal intelligence; and
- **Monitoring and review**: Firms should ensure that ABC controls are subject to regular and comprehensive assessments to promptly identify instances whereby the firm has failed to act in accordance with their own principles/policies/codes of conduct as well as applicable laws or regulations. Remedial action should then be taken accordingly.

FOR MORE INFORMATION:

RICHARD WEIGHELL
Partner

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

www.bdo.co.uk

42020160