INTERNAL AUDIT SUPPORT

BANKING & BUILDING SOCIETIES UPDATE

September 2022

IDEAS | PEOPLE | TRUST

BDO

BDO FS INTERNAL AUDIT CONTACT POINTS

Over the recent summer weeks, we've taken the opportunity to reflect on some of the common "lessons learned" reported by our clients in the course of our engagement work. This edition of our monthly pack explores these lessons to consider what Internal Audit teams should be thinking about for their own activities.

****

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

Click on a section below to take you straight there

ROLE OF INTERNAL AUDIT WITHIN TRANSFORMATION PROJECTS: LESSONS LEARNED

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

As part of our "Lessons Learned" edition of this monthly update, I wanted to share some insights from a recent presentation I delivered to the IIA Audit Leaders event regarding the internal audit of transformation projects.

What is unique about transformation projects?

- They are big and complex – buts that's not unique;
- They are forward looking – again, not unique;
- More significant, a true transformation project seeks to have a wide impact and, in many cases, impacts virtually every part of the firm;
- **But the major thing that stands out is that most transformation projects fail.**

What do transformation projects fail?

- The good, or legitimate, reasons are that transformation projects are genuinely complex:
  - Lots of moving parts, people to take along, and assumptions made;
  - The projects draw heavily on the skills of people who struggle to give the appropriate time commitment; and
  - There are uncontrollable elements, like loss of key people, market disruption or new regulations. These can be risk assessed and planned, but businesses are always going to be running some risks.
- But for the projects that go horribly wrong, often it is the bad reasons that play a major part:
  - Egos come into play. The benefits are overstated to get the project over the approval line;
  - Project leads have an optimistic bias. They want it to succeed, so they unconsciously overplay the positives and downplay the negatives;
  - People take on tasks for which they don't have the appropriate expertise or experience to successfully complete, driven by over-optimism;
  - When things get difficult, and progress slips against unrealistic deadlines/milestones, shortcuts are taken with little to no risk assessment;
  - Issues get considered individually and the holistic impact of such issues, and their impromptu solutions, is missed;
- So it is really important that transformation projects have someone with a cool head carrying out an objective review of the project. That's were IA comes in.

What should Internal Audit teams be thinking about?

- **Raise any doubts about the ambition of the project as early as possible**. If you have concerns, communicate your thoughts as soon as possible along with specific and measurable information about your concerns (avoid ambiguity, as this could misinterpret your constructive points as pessimism about the project). Request the project management team to demonstrate why they believe the project is feasible before the detailed project plans are prepared.
- **Both the Board and management want to have someone to give them a nod that the project is OK to go live.** If you allow the Board to make assumptions about the basis for IA's assessment of the project's risks, the Board can, and typically will, presume that the third line of defence has carried out more evaluation of the relevant risks than is the case. Even if the Board agreed the level of coverage the you were going to provide, you still need to be very clear regarding the basis of any risk assessment and draw the Board members back to discussion if you believe that the Board has over-estimated the level of assurance provided by the internal audit team.
- **Internal Audit has got to be clear that it is one part of the assurance framework and is there to provide a view, not a Go/No Go decision**. Position yourself very much as part of the three lines of defence. You can only provide a view based on the work you have directly undertaken to assess the relevant risks and the reliance you place on the assurance work of other teams, where such work is assessed to be reliable and competent. Your assurance map is critical.
- **Getting the business to focus on, and own, the risk assessment is vital.** If you find that the risk assessment isn't sufficient, focus more on improving the process for carrying it out than being the "source" for missed risks. The business must own the risks and the risk process.
- **All communications from Internal Audit need to be in the context of risk assessment and assurance plan.** It may appear a bit defensive, but it is vitally important that there is clarity on Internal Audit's role throughout the project.
- **Finally, if you are doing a mix of monitoring and assurance work, split your team so people only sit on one side**. It helps to maintain the objectivity of the monitoring staff, to distinguish the areas where there is assurance work and those where you are monitoring what management has given you.

ROLE OF INTERNAL AUDIT IN HORIZON RISK SCANNING: LESSONS LEARNED

BRUK WOLDEGABREIL
ASSOCIATE DIRECTOR
bruk.woldegabreil@bdo.co.uk
+44 (0) 7467 626468

While Internal Audit teams in regulated firms typically focus on the high risks driven by the regulatory and legislative developments affecting the business, some of the most severe, and often pervasive, challenges that firms face are non-regulatory in nature, e.g., shortage in skilled staff, extreme weather patterns, regional conflict, supply chain disruption, global cyber attacks, and the list goes on.

So the question is how well can Internal Audit enhance the firm's emerging risk assessment for such non-regulatory risks. Lets take pandemic risk as an example.

► COVID-19 – did you anticipate this in your emerging risk assessment?

Aside from the most ardent virologists, most of us did not predict the breadth, depth and longevity of the COVID-19 pandemic. As soon as we felt we mitigated the virus' impact by containing its spread and inoculating its worst impact on our health, we were hit by a variant of the virus, or repeat outbreaks – the road to recovery was uncertain and the UK has only recently moved from pandemic to an "endemic" situation (former UK Secretary for Health, 19 June 2022).

Most regulated firms likely had some form of "pandemic risk" on the risk register, typically flu strains we've previously experienced, e.g., SARs, avian or swine flu, with a model to consider different degrees of the pandemic's disruption to people, processes and technology. However, these (pre-COVID) risk assessments had some common human-based vulnerabilities worth considering for future emerging risk assessments:

- **Availability heuristic**: we tend to estimate the likelihood of an event occurring based mostly on our personal memory of past instances of that event. Unless your risk register is supported by objective analysis of historical trends assessment of future risk events will be incomplete and very likely flawed in supporting your efforts to prioritise risks.
- **Anchoring bias**: our assessment of risk is often heavily 'anchored' by the first piece of information we come across. A helpful technique is to separate information gathering from your analytical activities; take a look at the facts after the majority of the information gathering exercise has been completed.
- **Confirmation bias**: our natural cognitive tendency is to view facts and form conclusions that confirm our existing beliefs, e.g., "Pandemic prone viruses exist (risk), but serious outbreaks are rare (likelihood is low) and, thankfully, modern medical solutions have mitigated the most fatal diseases (impact is low) – our firm categorises this risk as Low in relation to other risks." Our perception of viruses before COVID-19 was driven by our viewpoint within developed economies, which have advanced healthcare and social welfare outcomes. We have to proactively challenge the basis of our modelling assumptions using external sources of information and incorporating different perspectives.
- **False consensus effect**: we generally believe more people agree with our view of the world and its risks than is the case as we tend to associate ourselves with family, friends and colleagues that buy into our consensus of thought. Its vital, in the pursuit of an independent and objective mindset, to sincerely seek differing perspectives. If you disagree with a perspective, challenge yourself to logically articulate why that perspective has an unsound basis or appears misinformed.

► What should Internal Audit teams be thinking about?

- Developing a risk register driven by the firm's known strategy, functional objectives and permitted activities is straightforward (in theory); attempting to identify external risks, entirely unconnected to the firm's operations, plagued by our innate human biases could appear to be an impossible task.
- However, rather than attempting to map every possible event that could ever happen, an appropriate strategy could be to open up your emerging risk assessment *process* to sources of information and perspectives beyond your immediate peer group and sector. Internal Audit teams should consider:
  - **Establishing a horizon-scanning working group within the firm**, drawing on staff from across the three lines of defence, to consider the current processes in place to identify sources of risk information. This helps incorporate information from outside the Internal Audit team;
  - **Sharing information and best-practice with Heads of Internal Audit** drawn from across your sector, for example, thematic events organised by the CIIA which also include subject matter expert speakers. This evolves your process by incorporating information from beyond your firm's perimeter;
  - **Membership to risk forums that gather views from the wider economy** and national security updates made available to the private sector. One example is the Centre for the protection of National Infrastructure (CPNI). The CPNI incorporates the impact of the National Security Strategy, National Risk Register and the UK's Counter Terrorism Strategy for regular risk updates and best practice guidance. Now your emerging risk assessment process can consolidate information from national and international sources;
  - **Partnering with external experts**, such as qualified advisors and professional futurists, that can entirely challenge your established emerging risk assessment process and facilitate a broader consideration or risks through advanced research and modelling tools not typically developed by regulated financial services firms. This further step could substantially enhance the value that the IA team provides through the business-wide risk assessment and help evolve the firm's broader approach in considering its resilience.

ECONOMIC CRIME UPDATE

SONIA DOHIL
MANAGER
sonia.dohil@bdo.co.uk
+44 (0) 7570 355038

September brings in new amendments to the UK's Money Laundering and Terrorist Financing Regulations (MLRs) - (Amendment) (No 2) Regulations 2022 (SI 2022/860) (SI). This included amendments and updates in relation to Proliferation Financing, reporting of material discrepancies to the register of overseas entities, and access to suspicious activity reports by the Regulator.

► What are the key changes?

- Firms are now required to assess their risks of proliferation financing. This is in addition to the existing obligations firms have for money laundering and counter-terrorist financing.
- Firms are now required to obtain proof of registration for certain types of overseas entities on the register of overseas entities (ROE). The register records the beneficial ownership of UK properties and firms have to report any "material" discrepancies they identify to the register. This obligation is in addition to the responsibilities firms have in place for the register of persons of significant control (PSC Register) and Trust Registration Service (TRS), where firms are also required to report "material" discrepancies. In addition, the responsibilities to report material discrepancies now apply on an ongoing basis, not just to discrepancies identified at onboarding.
- The FCA now has access to suspicious activity reports (SARs) submitted to the National Crime Agency (NCA). The sharing of SARs with AML supervisors, such as the FCA by the NCA is through a dedicated 'gateway'.

► What should Internal Audit teams be thinking about?

- **Proliferation financing:** firms are required to complete a proliferation financing risk assessment for their business. This could be either undertaken as a standalone assessment or integrated into the firm's business wide risk assessment. Firms should also review and consider the National Risk Assessment of Proliferation Financing 2021 as part of this process. Once completed, the outcomes of the proliferation financing risk assessment should be embedded into the firm's policies, procedures and economic crime controls framework. Firms are expected to take these steps, even if their exposure to proliferation financing is limited; this requirement is in addition to those existing AML and CTF obligations.
- **Register of overseas entities**: for those firms which deal with overseas entities, policies and procedures will need to be updated to capture the new reporting requirements for the identification of "material" discrepancies for beneficial owners of UK properties. Firms should also consider whether there are additional training needs for those responsible for the identification and handling of the requirement.
- **FCA access to SARs:** firms are not required to make any changes to their reporting requirements, but should be aware that there maybe additional discussions with the FCA where a SAR has been submitted to the NCA.

The Wolfsberg Group has published a guidance paper: Transaction Monitoring Request for Information (RFI) Best Practice Guidance. The purpose of the guidance is to provide best practices for correspondent banks using RFIs in the transaction monitoring process, i.e. help correspondent and respondent banks to better understand the risks of dealing with each other. It can also be applied to other payments-based relationships that firms may deal with.

► What does the guidance paper cover?

- The purpose of the guidance is to improve the awareness about the value of RFIs, help firms to understand how RFIs should be handled, and reduce the risk of ineffective or incomplete RFI responses which can lead to increased compliance costs.
- The paper covers roles and responsibilities within the process, timelines and expectations and a section on actions on insufficient/non-responses and how to deal with them.
- The paper further includes a comprehensive list of frequently asked questions during the RFI process and expected response from the respondent. The list of RFI questions serves as a guide only and is not intended to be a prescriptive list of mandatory questions to be asked by correspondent banks.

► What should Internal Audit teams be thinking about?

- The FCA has recently reaffirmed its expectations of firms' Anti-Money Laundering and Counter Terrorist Financing controls in relation to correspondent banking. Therefore, firms offering this service need to ensure that they are paying sufficient attention to industry best practice publications such as the new Wolfsberg RFIs guidance.
- In a correspondent banking relationship, one of the primary risks for the correspondent bank is its ability to monitor the respondent's transactions to detect any unusual or potentially suspicious activity. Firms, therefore, need to ensure that their transaction monitoring arrangements account for RFIs to be sent to their respondents. The more information that can be obtained via RFIs as part of the transaction monitoring process, the more comfort can be obtained in understanding the purpose of a payment or a set of payments. RFIs also evidence the respondent's ability to manage risk and provide comfort around its controls to the correspondent bank.

FOR MORE INFORMATION:

RICHARD WEIGHELL

+44 (0) 7773 392799
richard.weighell@bdo.co.uk

www.bdo.co.uk