April 2017
RECENT ('BUSINESS-AS-USUAL') INSIGHTS – LEARNING LESSONS AND AVOIDING COMMON PITFALLS

With a raft of regulatory change on the agenda, and Brexit on the horizon, **it is all too easy for focus to be unwittingly diverted away from business-as-usual (BAU) operations**. However, any firm that does take its eye off the BAU ball runs a real risk of regulatory intervention and potentially serious repercussions - the Regulator will likely have little sympathy in such circumstances.

This note consolidates our recent market observations and insight - through a BAU lens - on current themes, trends, areas of particular regulatory focus, lessons to be learnt and common pitfalls. The questions posed at the end of each section are intended as a practical framework by reference to which firms can benchmark their own positions.

The (inter-related) topics covered include:

- Heightened regulatory focus on the first line of defence
- Demarcation of responsibility between first and second lines of defence
- Importance of the 'need-to-know' principle
- Training and awareness – fit for purpose?
- Keeping abreast of regulatory developments and expectations
- The importance of demonstrability
- Delegation

Heightened regulatory focus on the first line of defence

The Regulator has for some time been keen to emphasise **the importance of the role played by the front office[1] in identifying and managing risk and, more generally, promoting a strong risk culture**. This comes against the backdrop of a perceived historic over-reliance within firms on the second[2] and third[3] lines of defence.

The Regulator's focus on the first line has become especially evident during supervisory visits – with front line personnel often constituting the majority of interviewees selected by the Regulator.

In essence, the Regulator is keen to ensure that those within the front office are demonstrably aware of, and alive to, the risks inherent within their respective business areas; together with the attendant controls implemented to mitigate those risks. **Fundamentally, risk identification and control is seen as a core and key responsibility of the front line**; and those within the first line should therefore be readily able to articulate their risk-related responsibilities**.**

Interestingly, some firms have now instituted dedicated first line risk teams, embedded within the business – and intended to provide more effective 'on the ground' risk management. We suspect that this may become a more prevalent feature over time.

[1] The so-called 'first line of defence'.
[2] Broadly, the control functions: Compliance and Risk.
[3] Internal Audit.

Questions

- Can front line personnel readily articulate their risk-related responsibilities and their role within the 3 lines of defence model?
- Are there areas in which the first line persistently seeks to abrogate its responsibilities to Compliance or Risk?
- Does risk management (and related expectations) feature prominently in training programmes?
- Do desk heads / managers demonstrably advocate the importance of, and assumption of responsibility for, risk management within their respective front line teams?

Demarcation of responsibility between first and second lines of defence

On a related note, many institutions will, in certain quarters at least, suffer from a **blurring of boundaries between first and second line responsibilities**. Accountability or expectation gaps represent an obvious risk, with important issues inadvertently overlooked and left unresolved.

Needless to say, any identified instances of blurred or opaque responsibility allocation should be promptly addressed. This is likely to require the clarification of accountabilities – whether through the modification of job descriptions, revisiting aspects of the governance and controls framework, provision of tailored training, or otherwise.

More cautious institutions will not be prepared simply to wait for an issue to materialise to discover the existence of an accountability gap. A more proactive approach might involve periodic interview-based Internal Audit and/or external consultant reviews – designed to highlight any apparent responsibility allocation / assumption issues.

Questions

In addition to the questions in the above box:

- Have any identified accountability gaps been satisfactorily addressed? Are there any on-going concerns?
- Does training adequately cover roles, responsibilities and expectations within the context of the 3 lines of defence model?
- Are job descriptions sufficiently clear on risk management responsibilities and expectations?
- Should the firm take a more proactive approach to the demarcation of responsibility?
- Would the firm benefit from a concerted focus on this area from Internal Audit or an external consultant?

Importance of the 'need-to-know' principle

The vast majority of firms will operate a ‘need-to-know’ policy – whereby sensitive information is required to be appropriately contained and its disclosure strictly limited to recipients who 'need to know' that information. However, adherence to this principle can be extremely patchy across firms and within an organisation.

It has become evident that **the Regulator has of late renewed its focus on 'need-to-know'**. For example, difficult questions are increasingly being asked of firms who, at the Regulator's request, produce insider lists which are of an inordinate (and inexplicable) length. Similarly, the Regulator continues to voice concerns[4] over the seemingly carefree way in which sensitive information is seen to be shared – whether involving the unnecessary disclosure of client confidential information at 'open' internal meetings, or of the entire contents of the Restricted List to the Dealing desk, or otherwise.

Against that backdrop, several institutions have stepped up their monitoring activities in this context – to ensure that 'need-to-know' really is the rule and not the exception.

Questions

- Is compliance with the 'need-to-know' policy actively monitored? By whom?
- Is internal awareness of the importance of 'need-to-know' sufficiently high and widespread? Do staff really understand what it means and what is expected of them? Are policies, procedures and training clear on expectations (including inadvertent disclosure/receipt)?
- Can the length of all insider lists maintained within the firm be objectively justified?
- Do physical arrangements support (or hinder) the operation of the 'need-to-know' policy. Would they withstand scrutiny of the Regulator during a floor-walk?
- Are supplemental controls in place in respect of the containment of 'inside information'? When were these last reviewed?

Training and awareness – fit for purpose?

There has been a **recent discernible trend towards more frequent, higher-quality and appropriately tailored training for relevant personnel**. Most firms will employ a combination of computer-based modules (often with an assessment component), supplemented by practical and interactive face-to-face sessions. Topics will typically include, amongst others: anti-money laundering; market abuse; conflicts of interest; anti-bribery and corruption; approved person refreshers; and Code of Ethics. In particular, **scenario-based workshops** have become a recurrent feature. In our experience, **realistic true-to-life scenarios** will generate the most interest and engagement; and maximise the overall utility of the sessions.

The inherent value – to both firm and individuals – of good training cannot be overstated. For firms, training constitutes an important control and helps to protect brand, regulatory standing and reputation, by ensuring a continued state of general awareness of important matters. High calibre training should also serve to equip attendees with the necessary knowledge and intuitive sense to identify issues before they materialise and to 'do the right thing' at all times. Equally, it should also preclude any miscreants from being able to plead ignorance.

Conversely, poor (and/or largely irrelevant) training is likely to be counter-productive; and may well result in a negative mind-set towards future sessions. Such an outcome would not sit well with the need for a strong institutional compliance culture.

[4] See, for example, in TR 15/13 (Flows of confidential and inside information).

Questions

- Are Management alive to the need for, and generally supportive of, a high-quality training programme?
- Is training overseen from the right levels of the firm's governance structure? Is it taken sufficiently seriously and regarded as a key form of risk control?
- When did the firm last review the quality and quantity of training? Was constructive feedback sought from participants? Is training content and delivery sufficiently 'real-world' and practical in focus? Does it engage the audience or perpetuate a negative mind-set towards all forms of education and awareness? Is it kept 'fresh'?
- Have any issues occurred which suggest that training provided may have been inadequate? How was this dealt with?
- Is training provided at appropriate intervals? When was this last considered and by whom?
- Is the firm aware of the full range of training available in the market? Or has the firm been relying upon the same providers year on year?
- Does the firm make sufficient use of interactive face-to-face training?

Mandatory means mandatory!

Training records are commonly requested by regulatory supervisors. It is especially important that all training designated as 'mandatory' is monitored to identify which relevant individuals have and have not undertaken the necessary course(s) or module(s). The Regulator may view anything less than a 100% completion rate as a 'red flag'; and potentially indicative of a poor institutional compliance culture. Notwithstanding, it appears that partial non-completion remains a relatively common phenomenon.

For firms with hundreds or thousands of employees, this can present a particular challenge – requiring **a disciplined record-keeping and follow-up protocol, with escalation processes and meaningful non-completion sanctions**, as necessary.

For mandatory face-to-face training, many firms will ensure that one session is recorded – so that any relevant individuals not able to attend in person can subsequently observe the session at a more convenient time[5].

Questions

- Does the firm maintain comprehensive training records, which it would be comfortable sharing with the Regulator?
- How does the firm ensure that all relevant personnel have satisfactorily completed mandatory training?
- Are all instances of non-completion dealt with robustly and escalated if necessary?
- Are there meaningful repercussions for those who fail to complete? Is this widely known across the firm? For example, will non-completion be a relevant factor in an annual appraisal / 'fitness and propriety' assessment?

[5] This can typically be tracked.

- Does the firm adopt a consistent approach to non-completion – regardless of the status and authority of the individual(s) concerned? Or are the 'C Suite' afforded special dispensations? If so, can this be readily justified?

Keeping abreast of regulatory developments and expectations

Firms are expected to keep fully abreast of all relevant regulatory developments and stated expectations – no easy task in today's fast-evolving regulatory environment. Practically, this will involve closely monitoring for any pronouncement – for instance, a final notice, thematic report, policy statement or speech – which may have **direct or indirect 'read-across' application** to their business and operations. It is not uncommon for, say, thematic reports specifically pertaining to a particular topic and sector to contain a statement to the effect that *all* firms should consider the extent to which the findings might also apply in their respective contexts. Accordingly, every firm will thereafter be regarded as 'on notice' of such expectations.

Further, it is notable that in a number of recent enforcement cases, the defendant firm has been specifically criticised for failing to pay heed to previously-published enforcement notices, involving analogous issues (notwithstanding that the nature of the firms' underlying businesses might have been very different).

Many larger institutions will now employ a dedicated 'Regulatory Developments' team, whose principal purpose is to monitor for, and ensure the appropriate internal dissemination of, relevant developments.

Once the import of a pronouncement has been assessed, a determination will need to be made as to what, if any, responsive actions are or may be required. In practice, this will often take the form of a 'gap analysis' exercise, designed to highlight any potential areas in which the firm is falling short of expectations. Ideally, any such exercise should be conducted by a suitably knowledgeable and independent function to ensure a truly objective and non-defensive assessment. The output should then be duly considered at the appropriate level within the firm's governance framework.

Questions

- How does the firm monitor for relevant regulatory developments? Does this provide a high level of assurance that all relevant pronouncements will be identified and, if necessary, actioned? Has this been objectively tested?
- Does the firm routinely track: thematic reports; final notices; upper tribunal decisions; regulatory speeches and occasional papers; policy statements; the Regulator's annual business plan; and regulatory Q&A publications?
- Have there been any known instances where a particular relevant development was not identified?
- Who determines how (and to whom) relevant pronouncements are disseminated internally? Do they have the requisite in-depth knowledge of the firm's business and operations to identify potentially relevant issues? When was this process last reviewed?

The importance of demonstrability

As has become increasingly apparent over recent years, **the importance (for both firms and senior individuals) of being able to evidence actions taken, discussions held or considerations taken into account, cannot be over-emphasised**. In practice, such evidence is likely to take the form of contemporaneous notes or other form of 'tangible' audit trail. A mere oral assertion is unlikely to carry much, if any, credence with the Regulator.

In a similar vein, many firms have been revisiting the manner in which formal meeting minutes are recorded – with a particular focus on ensuring that the minutes are appropriately reflective of: (a) all customer/client-related considerations and discussions; (b) all risk management issues addressed; and (c) meaningful challenge.

Questions

- Do formal minutes sufficiently and routinely reflect (a) to (c) above?
- Would the firm benefit from introducing a documentation protocol – to ensure a consistency of record-keeping across the organisation?
- Is there a perceived over-reliance on the mere fact that an event or discussion occurred; and consequently an inadequate focus on contemporaneous recording?

Delegation

Delegation is a prevalent and necessary feature within any financial institution. While responsible delegation has long been a regulatory expectation**, it is clear that the Regulator's focus is sharpening**. If evidence were needed, the UK Senior Managers & Certification Regime contains a specific conduct rule requiring designated Senior Managers to take reasonable steps to (broadly): (i) delegate appropriately; and (ii) to oversee the delegate effectively.

Conscious of the need to be able to demonstrate actions taken (if ever challenged), many senior officers are introducing an additional degree of discipline and formality into their meetings with direct reports and any other direct delegates. While this does not of course mean recording verbatim minutes of all such dialogue[6], it may for instance involve a summary bullet-form follow-up email, confirming what issues were discussed and any action points, timelines and accountabilities arising.

Questions

- Are senior officers sufficiently aware of the need to be able to **evidence** their effective oversight of delegates; and that this represents an obvious area of personal regulatory exposure?

In conclusion

The risk of allowing the multitude of regulatory developments to distract attention and resource away from BAU activities has arguably never been greater. However, prudent firms will neglect BAU at their peril.

[6] As this would not be workable, in practice.

This note has highlighted some of the observed themes, trends and potential pitfalls for firms in the context of BAU – all based upon recent experiences. The related questions can be used to help identify any potential areas of vulnerability or weakness; and to provide a gauge of BAU risk profile.

For further information contact, please contact:
David Berman
Partner
Financial Services & Regulation
London
One Fleet Place | London EC4M 7RA | United Kingdom |
Phone: +44 20 7653 2280 | Fax: +44 20 7653 2100
davidberman@quinnemanuel.com
Resume