

Senior management responsibilities – review time!

(This article first appeared in *The Compliance Institute Gazette*, Issue 178, June 2010)

The Financial Services Authority has recently imposed a financial penalty of £140,000.00 on an online provider of foreign exchange services for speculative trading, for failing to have in place adequate anti-money laundering systems and controls.

- The firm's former money laundering reporting officer (MLRO) has also been personally fined £14,000
- Specifically, the FSA imposed the penalty on the basis that the firm breached FSA Principle 3 and FSA Principle 7 – relating to failings in the adequacy of the firm's anti-money laundering systems and control

The fact that the FSA is flexing its muscles for breaches of control processes should not come as a surprise to firms. It is an FSA regulatory requirement that a 'firm must take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime'¹ Examples of other fines imposed on a variety of firm's include:

- "Deficiencies in compliance resources, policies, procedures and training, brought to attention of senior management but no remedial steps taken" (Major investment bank - £900,000 re inadequate market abuse training),
- "Failed to conduct its business with due skill, care and diligence in planning, authorising and executing strategy" (Major investment bank - £14,000,000 re distorting government bond market prices)
- "Financial services provider £49,000 and its money laundering reporting officer (MLRO) £17,500 for not having adequate anti-money laundering systems and controls in place for verifying and recording clients' identities."

Due to such risk and control failings in the financial services sector, the FSA has conveyed a number of consistent messages in the form of public statements, made through senior FSA and key staff, including that of Margaret Cole, Director of Enforcement, who earlier this year stated;

"The FSA expects senior management to take responsibility for ensuring firms identify risks, develop appropriate systems and controls to manage those risks, and ensure that the systems and controls mitigate the risks in practice. Failure to manage risks properly is now, more than ever, likely to result in disciplinary action being brought against individuals as well as firms. Senior managers need to understand this and ensure that they are taking appropriate action to identify and mitigate risks to protect their firm, and increasingly, themselves."

Such messages have been recently endorsed through FSA publications, such as the Annual Risk Outlook and its annual business plan. In terms of practicalities, there are a range of key questions that the FSA is likely to ask during a visit to a firm, albeit an ARROW visits and/or

cultural visit. The type of questioning is likely to address (but not be limited to) key themes such as terms of oversight, delegation and reporting lines. Below are some examples:

- Does the Board and management team have a “terms of reference”
- How does the firm evidence that oversight continues when responsibilities have been delegated, particularly when oversight is from Ireland?
- Is such delegation appropriate and are job descriptions current?
- Have responsibilities been clearly allocated?
- Are reporting lines appropriate and clear?
- What do dotted reporting lines mean in reality?
- What records are kept of all of the above?
- When were all of the above last reviewed?
- What training is in place to ensure employees know what to do in their roles – and how is its effectiveness measured?

The FSA, however, does not intend to tell firms how to run their businesses.

Common pitfalls for firms can include:

- Failure to demonstrate good corporate governance, even when it exists
- Job descriptions do not reflect reality
- Unclear allocation of responsibilities
- Delegating responsibility is not delegating accountability
- Management unaware of the information it should expect to receive
- Failure to review changes in risk profiles
- Being unaware of FSA’s hot topics and changing expectations
- Inappropriate oversight and delegation
- Training that does not focus on what employees should do differently in their roles to minimise risk
- Poor record keeping and more poor record keeping

In setting the direction of compliance and risk management strategy, it is clear that firms must apportion responsibilities among their directors and senior managers². This does not mean, however, that of a firm’s employees, only they are expected to identify, manage and mitigate risks; rather that whilst they have ultimate responsibility and will be held to account, minimising risk is the responsibility of all employees. This means that employees need to know what is expected of them in their roles. Having systems and controls in place to verify and record clients’ identities, to prevent money-laundering or market abuse, will clearly neither reduce risk nor satisfy the regulator unless employees have been effectively trained in their use, and are demonstrating not just competence in their use but the ability to apply them intelligently.

Of course, firms already deliver regulatory training annually to all their employees.

Or do they? In truth, training and learning are not terms that can be used synonymously. It does not automatically follow that because training programmes are delivered and evidence is collected proving their delivery, that learning has taken place, understanding and awareness have been raised, or risk has been reduced! When training does not fundamentally change employee attitudes and behaviours, and when it fails to provide them with heightened awareness of what alarms they should raise or when their suspicions should be aroused, then risk is unlikely to be mitigated.

So what can firms do to ensure that they have evidence their front-line employees have undertaken training, that learning has changed the way they work and that risk has been reduced?

Review the objectives of their firm's regulatory training. Strangely, firms' do not clearly articulate their objectives for regulatory training. It is left to subject matter experts to provide course content which tends to be a summary of everything they think employees should know about their subjects, rather than what they should do differently in their roles to mitigate risk. This results in technical and clinical content to which front-line employees, whose interests are often elsewhere, find it difficult to relate. Where objectives do exist, these tend to focus on what must be remembered rather than what must be done differently. Anti-money laundering training objectives emphasise the requirement to name the three main stages in the money laundering process; fraud prevention training objectives emphasise the identification of the three different types of fraud set out in the Fraud Act 2006. When objectives are defined in this way, employees quickly forget the content to which they have been briefly exposed. They may well be able to briefly describe placement, layering and integration, or provide short technical definitions of false misrepresentation, failure to disclose information and abuse of position, but their awareness of what might constitute a suspicious transaction, or what might constitute fraud may not have been raised at all. Defining objectives in terms of what firms want employees to do differently following training helps ensure that training content is meaningful and relevant and that employees are better equipped to protect their customers and the business as they go about their work.

Target the right training at the right employees. 'One size fits all' training provides comfort that all employees have been trained, yet it frequently fails to reduce risk either because it becomes diluted for specialists, or is so technical that it is inappropriate for front-line employees. Call centre employees, for example, need to be proficient in identification and verification and adept at not disclosing personal information to those who cannot prove they are entitled to have it. Conversely, employees in strategic procurement, for example, who negotiate contracts with potential data processors, need specialised training that may well embrace the implications of the eighth data principle, but that call centre employees are unlikely to require.

Make explicit the links between each of the firm's regulatory training modules. Often, information security, data protection, fraud prevention, anti-money laundering and other financial crime training are treated as separate 'subjects', each owned by different subject

matter experts. This means that the connections between, say, a failure to protect personal information and an increased risk of identity theft and financial crime, that are obvious to specialists are less so to front-line employees. Each subject becomes just another course making it more difficult for employees to understand the wider landscape and to see that their actions, (failure to protect personal information), have consequences, (identity theft and financial crime). To design regulatory training that has as its clear purpose, the reduction of risk, it is vital to see each 'subject' or 'module' as part of a coherent whole; each one building on and complementing the others, so that learning is re-enforced rather than fractured and then forgotten. Such an approach ensures that what employees learn is greater than the sum of the individual subject areas.

Measure the effectiveness of regulatory training. Sadly, few firms regularly measure the effectiveness of their regulatory training. Few Chief Executives, Directors or Senior Managers would sanction major IT projects without approving a robustly prepared business case and without expecting a real return on investment which can is not only measured, but is seen to be delivered. Similar robustness needs to apply to regulatory training; directors and senior managers should expect to see a sound business case for effective training and a return on investment that is linked to the business' objectives, strategies and goals to identify, manage and mitigate risk.

¹ The FSA Handbook, (Senior Management Arrangements, Systems and Controls). SYSC 3.2.6R

² The FSA Handbook, (Senior Management Arrangements, Systems and Controls), SYSC, 2.1