Ten Top tips for managing compliance

Peter Scott

Outcomes - focussed regulation (OFR) has now been with us for nearly four years and during that time I have seen firms, both large and small, put in place a multitude of procedures to try to manage their compliance risks. Sometimes these have been carefully planned and implemented and as a result, tend to be more effective. However from what I often see, compliance measures in many law firms have not been based on any *comprehensive planning* but have been developed on an 'ad hoc' basis. Moreover, the procedures which are put in place are more often than not inadequately managed and observed in practice.

My experience has also been that some firms only wake up to the inadequacy of their risk and compliance measures when something goes wrong. For example, since the beginning of this year I have seen a succession of problems arising from breaches of personal data security and this has in turn made the firms affected far more aware of how little they and their people understand DPA issues and the steps they should have been taking to protect client data. The good outcome has been that as a result of such problems, a 'kick start' has usually been given to a review of their overall management of risk and compliance.

I would suggest that it is now time for firms to take stock of how they manage their risks and compliance and for this purpose I will share with you my *ten top tips* for managing compliance.

1. Review the resources required for effective compliance

For many firms risk and compliance management has not been (and is still not) a top priority, and as a result it is often a seriously under-resourced area of operation. The resources applied to managing it in some firms I have observed are likely to be no more than a few hours a week (if that) spent by the COLP, COFA and MLRO.

In order to put in place and effectively manage compliance, a firm will at the outset need to scope the functions required for effective compliance before it can establish what resources are needed and how they should be applied. Resources in a law firm are limited – people, their time and money.

While a firm cannot 'outsource' for example, the roles of COLP, COFA and MLRO, it can and ideally should build **teams of people** around them to help them with their roles, because one person alone will not be able to effectively carry out each of those roles. Should a firm put a team together using internal people or should it buy-in resource from external sources? Likewise, should a firm consider using partners to assist a COLP for certain functions or should it buy-in a professional compliance manager, as many larger firms have done? Cost of course may be a factor in this decision and a firm should consider whether it is better value for money to buy-in a professional compliance person instead of using an equity partner who is likely to be more expensive and have less time to do the job effectively.

To enable a firm to plan its required compliance, I would suggest carrying out a cost/benefit analysis in respect of every aspect of risk and compliance management to establish **the most resource effective** method.

2. Review your higher risks

Firms ought to know, because of the nature of their work or their past risk and compliance experiences, which are the higher risks for them. For example, money laundering, cyber fraud and

client account problems may be high risk areas for a firm because of an extensive conveyancing practice or other nature of its work and I have already mentioned increasing problems with loss of client data. Likewise a series of complaints (whether or not they have reached the Legal Ombudsman) should ring warning bells to tell a firm it needs to get its client care and complaints handling into better shape.

However, a review of high risks for a firm should not be limited to what is perceived as 'SRA compliance' – it should extend to every type of risk which can impact on a firm, including –

- **Operational risks**, involving the risk of negligence.
- **People risks**. People are a law firm's greatest asset but are also a firm's greatest risk.
- **Other regulatory risks.** There are many other regulatory risks with which law firms must comply in addition to SRA regulations.
- **IT risks.** It is difficult to conceive of a law firm today without IT, but if the IT fails it can be disastrous for a firm.
- **Financial risks.** Financial stability is a mandatory outcome
- **Assets risks,** which require firms to have effective disaster recovery plans in place.
- **Reputational risks.** If a law firm has its reputation damaged it can spell disaster (remember Anderson).
- **Management risks**. If management does not know a firm's risks and is not in control of those risks, then the firm is seriously 'at risk'.

A firm should prioritise a review of its risk areas using 'risk mapping' techniques and begin by focussing on those risk areas likely to involve 'high incidence and high impact'. Using its existing risk and breaches registers, a firm should review whether in each risk area it has adequate measures in place to -

- Identify and assess those risks;
- Effectively control those risks;

3. Put in place pre-file opening risk assessments.

Does your firm have pre-file opening risk assessments and if so, how effective are they in preventing you taking on high risk clients and matters?

Many, if not most of the highest risks to law firms arise from taking on work and clients without adequate risk assessments being carried out. Many firms still leave control of taking on matters and clients solely to the judgment of individual partners and other fee earners. However, experience has shown that the judgment of some people in law firms is less than adequate. Risk assessments should ideally highlight risk factors for a firm which need to be scrutinised and assessed. Depending upon the assessment made, a decision as to whether or not to take on a matter will need to be taken and if a matter is taken on, it will also need to be decided not only how that matter will be managed and supervised, but also how identified risks will be factored into the pricing of the job.

4. Review the effectiveness of your measures to manage risks and compliance.

Unless the effectiveness of its risk control procedures is monitored and measured on a continuous basis against pre-set objectives , a firm will never know the incidence and extent of its risks and non-compliance. Ideally a firm's approach to monitoring and measuring the effectiveness of its risk procedures should be systemised using its IT systems to embed common risk management

procedures into an IT framework to provide an integrated and cost-effective way to streamline the monitoring and assessment.

The effectiveness of its techniques designed to reduce or eliminate risks and to identify residual gaps should be tested on a regular basis. Ideally such techniques should include the following –

- **File reviews and audits** by experienced people within a firm or by external reviewers should be an integral part of a firm's risk management strategy.
- **Claims monitoring**. Recording and analysing claims of negligence (and circumstances which may lead to a claim being made) against a firm are likely to be as good an indicator as any that operational risks are not being managed as they should be. This will also indicate the steps required to be taken to reduce exposure for the future and the manner by which such risk management measures should be continuously monitored and assessed.
- **Complaints monitoring**. Recording actual complaints made against a firm, as well as expressions of dissatisfaction by clients is necessary if their causes are to be identified, analysed and risks associated with them assessed, so a firm can take preventative steps for the future.
- **Supervision** of people by those in a firm who are appropriately experienced and qualified should be seen not only as a means of risk prevention, but equally, as an effective way of monitoring and assessing the quality of advice against the standards of excellence required by clients.

5. Review the effectiveness of systems for internal disclosure of possible breaches

Attempts to drive internal disclosure of possible breaches of compliance and other risks can present particular difficulties for law firms. This will usually depend upon there being an open and 'no blame' culture so everyone feels able to report mistakes and problems. However, this can be difficult to achieve, despite there being 'whistleblowing' legislation in place. If no compliance breaches are being reported then that is unlikely to mean there are no breaches (because life in a law firm is just not like that!) and more likely to mean that there is probably a culture of fear.

On the other hand some firms have found that requiring partners and staff to positively confirm in writing that they have followed certain stated procedures can be very effective, particularly if combined with regular file reviews.

6. Review the effectiveness of your systems for reviewing incidents and reporting to regulators

It is vital that a firm has in place systems for reviewing incidents that have occurred which may constitute regulatory breaches and require reporting to the SRA or other regulators, as well the means to implement any necessary measures to ensure such problems do not re-occur.

Establishing a **risk committee** can be an effective way of dealing with this. The COLP and COFA and other risk and compliance people within the firm will be required to report all incidents and risk issues to this committee on a regular basis so that the committee will have a comprehensive overview of all risk matters impacting on the firm. The COLP (and also possibly the COFA) will be members of the committee and one of its most important roles will be to consider whether any matters need to be reported to regulators (or others, such as insurers). The committee needs to have the 'muscle' to implement and enforce any risk and compliance procedures it considers necessary.

Having a well-functioning risk committee is also likely to indicate to the SRA and other regulators that a firm is taking its compliance obligations seriously.

7. Review your risk and compliance training programme

Quality focussed training in relation to the risks to which law firms and their people are exposed is vital if everyone in a firm is to develop a sufficient level of awareness for them to recognise risk situations when they occur and to deal with them satisfactorily in a manner which protects clients, themselves and the firm.

Relevant training is about to become even more of a vital requirement for lawyers with the introduction of the statement of solicitor competence which will affect solicitors throughout their careers and is intended to be the yardstick by which solicitors should continually assess their own skills and identify knowledge or skills gaps. In future, solicitors will have to demonstrate an understanding and assessment of their own weaknesses against a set of principles, and COLPs will need to be involved in the development of training programmes designed to ensure that solicitors understand the new requirements, given the link between the statement of solicitor competence and Principle 5 (*you must provide a proper standard of service to your clients*). It was said recently by Martin Coleman, the chair of the SRA's education and training committee that '*Failing to take adequate steps to maintain your competence may be an aggravating factor in any disciplinary proceedings*" (Solicitors Journal, 21 April 2015).

Law firms should now use the competence statement to support their lawyers in achieving compliance with the new requirements and to ensure that everyone in a firm is clear as to how risks and compliance must be managed.

8. Make sure your management team 'buy-in' to risk and compliance and have the necessary skills

It is often assumed in law firms that those who are managing a firm are themselves good risk managers and are compliant in how they operate. Too often the opposite is the case.

Managers need to be totally aware of all the risks to which their firms are likely to be exposed. If however they do not possess the required knowledge of those risks or the skills required to enable them to identify those risks, then a firm and its people will be **'at risk'**. It is now not good enough for a law firm manager to say *"I don't do risk management"*. Likewise it is not good enough for a managing partner to say that the firm has a COLP or a professional risk manager to manage risk – the buck stops with the managing partner!

Ask yourself whether your managing partner and other managers in your firm are totally on top of the risks to which your firm may be exposed?

Earlier in this article (at 7 above) I recommended that firms now review and renew their risk and compliance training. If training is to be successful in building awareness and embedding a culture of risk management in a firm, then the managers in a firm must show others in the firm that they themselves believe in managing all the risks to the firm by *practicing what they preach*, otherwise others will not follow. Risk management must come from the top.

9. Review your governance procedures

In addition to having a management team that is prepared to drive a culture of risk management and compliance, it is also necessary to embed within firms appropriate governance arrangements to support management's efforts. For example -

- **A risk committee** as mentioned at 6 above.
- **A conflicts committee.** Conflicts of interests (whether own interest conflicts or client conflicts) are increasingly a problem for law firms, particularly as firms grow in size and complexity and where it is no longer possible for everyone to know what everyone else is doing and the clients they act for. Establishing a conflicts committee made up of a few senior and risk-averse members of the firm to which issues relating to potential conflicts of interests can be passed for decision can be a very valuable risk tool.
- **A reputational risk committee.** Likewise having a reputational risk committee to watch over all issues which could bring about damage to a firm's reputation (see 2 above) is another useful tool to have in the risk and compliance armoury. Any risk if it crystallises, can have a consequential impact and cause other risks to also crystallise and cause loss. And in particular, if any risk crystallises there can be damage to the reputation of a law firm. The demise of the accounting firm Anderson is perhaps the most striking example of this in the recent past.
- **'Risk issues' to be a standing agenda item at every management meeting.** Many well run firms have for a long time placed risk management high on their list of priority issues and included 'risk issues' as an agenda item at every management meeting (at my former firm we were doing this 25 years ago!)
- **Support for your COLP and COFA.** I would suggest that for the proper execution of the responsibilities of a COLP and COFA, the duties of Partners as are currently set out in their Partnership or Members' Agreement should be revisited, amended and supplemented by incorporating appropriate provisions relating to compliance, including:
  - Members/partners are obliged to comply with all the Principles, Outcomes, Rules and other requirements of the SRA Handbook and of all other regulation affecting the firm; and
  - Members/partners lend themselves to such procedures as are necessary on the part of Management and/or the COLP and COFA to ensure that the firm is at all times compliant and that they expediently and fully render all such assistance to Management and/or the COLP and COFA as may be necessary. Breach of the above obligations could carry sanctions such as suspension, involuntary retirement notice or expulsion.
- **Consideration should be given to incorporating a 'whistle blowing' policy**, such as is referred to in indicative behaviour IB (10.10) in the SRA Code of Conduct.
- **The COLP and COFA to have full access** as is required to all LLP/partnership information and documentation, including (if they are not part of management) the right to attend management meetings as appropriate.
- **Recognising that there may be differences of opinion** between management and/or partners and a COLP or COFA, as to aspects of compliance, the COLP and COFA should be indemnified by the firm/ LLP in relation to the execution of his/her duties, particularly to the extent that he/she becomes involved in penalties, costs or expenses.
- **It should be provided that the COLP and COFA are entitled to take independent external advice** at the firm's/LLP's cost where a compliance issue arises and that the firm/LLP and its members / partners agree to accept and implement such advice.
- **Consideration should be given to a provision for the resolution of disputes** as between the COLP/COFA and management and/or partners.

- **Training**. It would also be appropriate to provide that the COLP, COFA and others such as MLROs (and any 'deputies' the firm may wish to put in place to ensure continuity) should undertake at the expense of the firm such training as may be required.

10. Consider how to 'systemise' your risk and compliance monitoring

Providing the necessary resource to effectively manage compliance and other risks is a major issue for most (if not all) law firms. Cost effective ways to capture knowledge and more effectively monitor risks should be high on the agenda for law firms. How can the use of IT assist in this process?

IT is not a panacea to overcoming all hurdles to effectively managing risk and compliance, but it can be a very useful and powerful tool to –

- Create and maintain a central, up to date compliance and risk database;
- Provide information access to everyone who needs it in relation to exposure to risk and its management;
- Embed into a firm's systems, its compliance and other risk management procedures, such as client inception procedures;
- Streamline the identification, recording, assessment and mitigation of compliance and other risks, including exceptions to compliance;
- Demonstrate to insurers and the SRA that a firm is effectively managing its risks.

In addition to using IT to systemise risk management, I would also advocate adopting a *systematic approach* to risk and compliance to enable a firm to put in place a **formal** compliance and risk management process which incorporates for example, the following features -

- It is management driven from the top so that compliance and risk are seen to have management buy - in and are adhered to by everyone throughout the firm;
- A 'zero tolerance' approach is necessary – 'just do it!';
- Managing risk and compliance are seen as 'everyone's job';
- A 'no blame' culture is developed to encourage disclosure;
- Investment is made in training and education programmes to build awareness and to change mind-sets;
- The continuous challenging the effectiveness of compliance and risk procedures is implemented'

The advantages of a **formal** compliance and risk management process will:

- provide a structured approach to effectively prioritise and focus on the most appropriate risk and compliance areas;
- demonstrate the effectiveness of a firm's risk and compliance procedures and outcomes;
- ensure continuous monitoring which should ensure that the management of compliance and risk is 'lived' on a day to day basis; and

- help to provide comfort to professional indemnity insurers and hopefully the SRA in relation to how effectively a firm manages its risks and compliance.

Peter Scott runs his own professional consulting practice, Peter Scott Consulting.