Regulatory compliance for solicitors Part 2: Compliance planning

In the second part in this series looking at the new regulatory regime for law firms, compliance specialist Jonathon Bray offers some valuable insight and practical compliance planning suggestions for Compliance Officers for Legal Practice (COLPs) and Compliance Officers for Finance and Administration (COFAs).

In the first part of this series, the main themes running through the SRA Code of Conduct 2011 were identified, namely professional ethics, client care, risk management, financial stability and management of the business. In Part 2, the focus is on what firms and their Compliance Officers should be doing, or close to completing, in preparation for the 1st January 2013 when the new regime comes into force.

Under the new regime solicitors are for the first time required to self-regulate. The responsibility is focused upon the COLP and COFA, but the firm itself (including its owners and managers) remains accountable for compliance, and individuals within the firm accountable for their own behaviour. The Solicitors Regulation Authority (SRA) has been keen to repeat mantra-like that the Compliance Officers will not become 'sacrificial lambs' in the compliance cause. However, the majority of the administrative and management burden of compliance will fall on the COLP and COFA, and now is the final opportunity to settle the firm's compliance plan before the new roles 'go live'.

Compliance planning

The SRA clearly expects firms to produce something entitled "Compliance Plan", since it is referred to in the Authorisation Rules, though there is no further guidance about what a Compliance Plan should look like.

Many firms will use the guidance in the Authorisation Rules as the basis of the Plan, whilst other firms are taking a slightly different approach. They are using the Compliance Plan to document:

- a risk and compliance audit, to evidence that they have considered how compliant the firm was at a certain date and where the key risk areas and gaps lie;
- a prioritisation process of risks and compliance gaps, including a plan of action for managing the risks and closing the gaps;
- what the firm already does well, and which informal systems and controls should be formalised;
- who is responsible and accountable for particular compliance tasks;
- what will happen when things go wrong (processes for recording breaches and reporting internally and externally);
- what the key compliance systems, policies and procedures are and where they can be found;
- a timetable for reviewing the firm's compliance arrangements including key dates;
- an overall statement of the firm's approach to risk and compliance issues.

However the firm chooses to implement it, it is clear that a Compliance Plan is more than just an office manual. Whilst having a set of well-drafted and comprehensive policies and procedures is certainly important, it should not be relied on as the gold standard in compliance but rather viewed as a piece of a bigger jigsaw.

It makes sense that the Compliance Plan is highly visible rather than being a purely management document, so incorporating it into the office manual might be sensible. Some firms will put their Compliance Plan on the first page of the intranet, others will disseminate it via memo and email. Whatever approach is taken, it is incredibly important that the Compliance Plan is properly introduced to the firm, and that training is provided where appropriate.

Requirements of a compliance plan

Guidance note (iii) to Rule 8 of the SRA Authorisation Rules 2011 outlines the main requirements that a firm's compliance plan should cover, whilst making it clear that the individual plan will be dependent on factors such as the size and nature of the firm, its work and its areas of risk.

Common areas which should be covered include, amongst others,

providing a transparent framework for responsibilities within the firm, appropriate accounting procedures, appropriate systems for monitoring, reviewing and managing risks (including the giving of undertakings), and systems supporting the development and training of staff in matters of compliance.

Evidence of compliance planning

As well as the firm's statement on compliance, the Compliance Plan also becomes documented evidence that the principals in the firm and the Compliance Officers have carefully thought about what being regulated means for the firm, its clients, and its systems and processes.

In fact, some might argue that part of the real value of having policies and procedures written down is not so much in what they add by way of substance (many firms rightly point out that they are already doing much of what is required of them, albeit informally), but how this ensures that the firm's systems of compliance are documented and evidenced. If the regulator ever shows up at the door to ask what systems were in place following reports of a breach of the rules, it will be extremely important to be able to point to a clear, well-documented process.

Having said that, firms should avoid putting things in place simply to satisfy the regulator, and this for two main reasons. Firstly, it will be a waste of valuable time and resources — implementing a system and culture of compliance is not a quick and easy task, so that time will be better spent working towards ways of being compliant for the benefit of the firm and its clients. Secondly, the SRA's relationship managers will become more and more skilled at sniffing out bluff as time goes by. If they believe that firms are telling them what they want to hear, or worse, actively deceiving them, serious regulatory penalties and sanctions are likely to follow.

It is a key principle of the SRA Code of Conduct that lawyers must:

"...comply with your legal and regulatory obligations and deal with your regulators and ombudsmen in an open, timely and co-operative manner..."

So, if having a Compliance Plan and a set of comprehensive policies and procedures are not the silver bullet, what else should firms be doing?

Creating an audit trail

Creating an audit trail need not be an onerous or time consuming task, and the trail can be built into formalised systems if appropriate. By way of example of a formalised system, firms are likely to incorporate some form of peer file review as part of their supervision systems, and the audit trail might look something like this:

- COLP implements a supervision policy, recording training given to relevant staff in personnel files.
- A fee earner reviews 2 files per month on a standard file review form, copies of which are forwarded to the COLP.
- The COLP records which reviews have taken place, and what (if any) breaches of the rules or warning signs have been identified.
- The COLP makes an attendance note of any action taken to rectify breaches, including meetings held and training given to staff.
- The COLP raises more serious issues and trends as a risk to senior management.
- Breaches of the rules are reported to the SRA as required.
- The COLP spot-checks a number of file reviews to ensure they are being consistently carried out across the firm, recording which files have been spot-checked and any issues encountered.

However, not everything will fit neatly into a procedure and so COLPs and COFAs will be keen to emphasise that audit trails are to become part of the firm's culture.

Fee earners and Compliance Officers alike must keep accurate records of their compliance, including emails, attendance notes, memos, minutes and so on. The COLP and COFA in particular should ensure that their decision-making is clearly documented. Whether the decision concerns whether a particular matter can be taken on by the firm, or whether it is a judgement call on whether a breach of the rules is "material" (and therefore immediately reportable), evidence of the processes leading to the ultimate decision should be available for inspection at a later date.

Some firms will use sophisticated technology to help them create an audit trail, by producing reports and audits at the touch of a button which could potentially save fee earning time. The essential challenge for firms is to organise the ways in which the audit trail is created and information is stored, rather than necessarily trying to invent new ways of working and collecting information.

Capturing and analysing compliance data

Outcome O(7.2) of the Code of Conduct states that firms must have:

"...effective systems and controls in place to achieve and comply with all the Principles, Rules and Outcomes and other requirements of the Handbook, where applicable..."

These systems and controls will generate all manner of data that must be systematically recorded and analysed. In order to do these things, the data must first be captured and this may not be particularly straightforward, especially in larger practices, so will require careful planning.

Take a COLP's recording and reporting obligations by way of example. As a reminder, the COLP is required to take reasonable steps to record all breaches of the rules (except the SRA Accounts Rules) and report them to the SRA - either immediately in the case of 'material' breaches, or

(Continued on page 14)

(Continued from page 13)

in the annual information report for less serious breaches. This prompts the COLP to consider how, given the size, culture, personnel, and geographical spread of the firm, they will be made aware of these compliance failures. Putting in place formalised systems of reporting and audit is clearly important, and these steps will almost certainly uncover the most serious instances of compliance failures.

What is likely to be a bigger challenge for the COLP is generating data on the less serious (and arguably trivial) breaches. It is against human nature to self-report or tell tales on colleagues, particularly for something which is not classed as serious.

However, the Authorisation Rules make it clear that a pattern of minor breaches may become a material breach and, without the necessary data to analyse, the COLP will be unable to make that judgement call.

How will this challenge be overcome? Taking 'reasonable steps' to record compliance failures may well require more than implementing formalised systems and auditing performance. Other steps towards creating a more whistleblowing culture might include:

- firm-wide training on individuals' reporting responsibilities, with regular refresher sessions;
- effectively communicating the firm's commitment to quality and compliance;
- leading by example, with partners taking an active role in reporting;
- allowing failure to be used as a learning and development tool, rather than grounds for punishment;
- having a network of 'deputy' COLPs throughout the firm;
- operating general policies to make reporting less intimidating, such as an open door policy and a 'no guilt' policy for self-reported failures.

Of course, Compliance Officers must keep track of more than just compliance failures. Data may be generated in many different areas, such as risk assessment and negligence, complaints and client satisfaction surveys, training records and file reviews, conflicts of interest, referral payments, commissions or fee sharing, and suspicious client activities. Firms must consider how this data will be captured and, equally importantly, how it will be analysed.

Clearly, collection of the data will be just the first step in a longer analytical process. Compliance Officers will then scrutinise the data looking for trends, patterns and warning signs which will enable them actively to manage risks and comply with their reporting obligations. The aim of the Compliance Officer will be to have a thorough understanding of the firm's activities at any given time.

Conclusion

Most firms will have already begun the compliance-planning process and may even have implemented systemic changes as a result. Those who have not properly addressed the new responsibilities will need to do so urgently. The firm's current level of compliance should be carefully audited and a plan produced to address any perceived areas of risk, putting in place new systems of gathering and recording information where necessary.

Careful consideration should be given to how compliance data will reach the COLP and COFA, and how that data will be recorded and analysed.

Ten compliance tasks to complete before 1st January 2013

1. Analyse the business, its risks and compliance gaps - if changes are required, prioritise the high risk areas.
2. Write a Compliance Plan, and agree it at top level.
3. Consider entering into Compliance Officer Agreements with indemnities, and amending COLP and COFA job descriptions and employment contracts.
4. Speak to the firm's broker about COLP and COFA insurance.
5. Give unequivocal backing to the Compliance Officers and agree resourcing requirements and budgets.
6. Become an authority on the SRA Handbook 2011 (COLP), the SRA Accounts Rules 2011 (COFA) and other relevant legislation - there are plenty of training events and webinars available.
7. Review and update the office manual and other relevant policies and procedures.
8. Set up suitable data capture and recording systems - if planning to use software, get demonstrations from suppliers to ensure they fit with existing systems and work methods.
9. Set up a risk-management system involving a regular top level review of the risk register.
10. Train staff on the requirements of outcomes-focused regulation, their internal reporting duties, and any changes made to systems, policies and procedures.

Jonathon Bray
Jonathon Bray Legal Services
info@jonathonbray.com