

Changing direction

**Create a culture of
continuous innovation**

10 Questions: Ian Jeffery

How Lewis Silkin will succeed
without mergers

Pricing for value

Develop a winning value-based
pricing strategy

Human law

How soft skills will differentiate
lawyers from robots

MASTERCLASS

Bulletproof compliance

Frank Maher discusses how to ensure your law firm is compliant with relevant professional, legal, regulatory and client-imposed obligations

FOUR THINGS YOU WILL LEARN FROM THIS MASTERCLASS:

- 1 The key compliance areas that law firms should manage
- 2 How to benchmark your firm's performance against peer firms
- 3 How to implement a customised compliance system
- 4 Common problem areas in managing compliance

Many commercial law firms outside the UK and USA which are market leaders in their jurisdictions are at an early stage of developing their firmwide compliance programmes. Increasingly, however, firms are being pressured by clients to demonstrate their compliance systems in a range of areas, particularly information security and anti-bribery.

Every firm has more to do in this area – implementing a compliance programme is a journey, but it has no end point; there will always be something new to address.

Compliance requirements

What are law firms required to comply with? The list is long and includes the following.

- **The law, first and foremost.** Law firms are subject to the same laws as any other business and their professional obligations will require them to uphold the law.
- **Bar Association or Law Society rules.** These may not be confined to your local jurisdiction, but may extend to those applicable in other office locations. International codes may apply, such as the Code of Conduct for Lawyers in the European Union (prescribed by the Council of Bars and Law Societies of Europe) and/or the International Bar Association's International Principles on Conduct for the Legal Profession.
If the firm employs lawyers from other jurisdictions, they may also be subject to the rules of their domestic regulator. Key areas to consider include conflicts, confidentiality, independence and supervision requirements, but there will be others too. In England and Wales, there are specific requirements for risk management and complaints procedures.
- **Financial crime.** Anti-money laundering, counter-terrorist financing, anti-bribery and financial sanctions regulations and legislation apply to law firms. The extra-territorial reach of the US Foreign Corrupt Practices Act and the UK Bribery Act 2010 can be a significant

issue, with firms considered accountable for the actions of both their agents and joint venture partners.

Sanctions imposed by the US Office of Foreign Asset Control, the European Union and the United Nations have been among the most taxing areas for many firms over the past couple of years, particularly with the Arab Spring and events in Russia and Ukraine.

- **Data protection and information security.** This is frequently the most onerous compliance requirement of all. Client pressures may be brought to bear on their service providers and firms may be subject to auditing by specialist consultants. Professional obligations of confidentiality and, in many civil law jurisdictions, criminal sanctions for breach of professional secrecy obligations, are additional compliance dimensions to manage.
- **Client requirements/outside counsel guidelines.** These can be among the more onerous requirements, particularly when clients seek to impose wide conflicts rules which may go far beyond regulatory requirements.¹
- **Other law firms.** Some large international firms instruct law firms in other jurisdictions or recommend that their clients do so on



multijurisdictional work. While they may at one time have relied on a listing in one of the established directories or personal acquaintance (perhaps through meeting at international events), they often now impose more rigorous checks.

- **Insurance requirements.** These may arise directly or indirectly, as insurers' expectations are continually increasing. In future, the existence of appropriate compliance systems may be the passport to obtaining any professional indemnity cover. In some jurisdictions, insurance may not be required, but firms doing international work are likely to find at some point that clients expect it.

“There may be a difference between what senior management say happens and what actually happens on the ground”

- **Unauthorised practice of law.** In England and Wales, where the ban is not as broad, this is known as engaging illegally in ‘reserved legal activities’. Restrictions on who can provide legal services at all or what services they can provide without local qualification vary considerably around the world. Some countries' laws even restrict visiting lawyers from providing ‘fly in, fly out’ advice on the law of their home state.
- **Confidential trading information.** Price-sensitive information/insider dealing legislation may apply, breach of which may carry criminal sanctions.
- **Sarbanes-Oxley.** Rules under the US Sarbanes-Oxley Act require an attorney to report evidence of a material violation of securities law or breach of fiduciary duty or similar violation by the company or any agent of it to the chief legal counsel or chief executive officer of the company. If an appropriate response is not received, the attorney must report the evidence to the company's audit committee or to the board.

In addition to the above, firms also need to manage their risk of professional liability claims. Indeed, the roots of many US law firms' compliance systems can be traced to the appointment of loss prevention partners or general counsel and the establishment of supporting risk management systems. In the UK, these have gradually been rolled out since approximately 2000, coinciding with the demise of the Solicitors Indemnity Fund, the profession's monopoly statutory insurer.

Benchmarking compliance

The starting point in benchmarking your firm's performance relative to its peers is to conduct a gap analysis to establish where the firm stands in terms of compliance compared to where it needs to be. Most firms have some risk management systems which have been built up over the years. However, these have often been designed to address specific issues and are not comprehensive.

A structured approach to identifying a firm's current position should start with a review of written procedures. This can then be followed by interviews with key individuals – not just the managing or senior partner and the partners who head practice areas, but also others in management positions with responsibility for support services, such as human resources, information technology and accounts and finance.

Much will depend on the size of firm – in a small firm, one person may have responsibility for more than one of these functions. In a larger firm, there may be a risk and compliance team which should also be part of the process.

Interviews will help to understand:

- the firm's client base (client type, sectors, geography);
- how each practice area works (client engagement, conflicts, anti-money laundering, etc);
- supervision;
- culture; and
- risk and compliance processes.

But, there may be a difference between what senior management say happens and what actually happens on the ground. There are two ways of building a bigger picture – either by interviewing a selection of fee earners and support staff, or by online testing. Support staff can be an invaluable source of information.

Online testing, such as through Legal Risk's *Desktop* risk diagnostic tool, can also be invaluable, as it results in information being obtained from a wide cross-section of staff. Because the responses are usually provided confidentially, it encourages staff to be more open. The tests provide results in graph form, which provide a readily-digestible report that can be benchmarked against peer firms (anonymously, of course).

Recent testing of staff in one leading law firm using this tool showed that:

- 65 per cent did not understand financial sanctions and the firm's procedures to manage them;
- 73 per cent did not understand their anti-money laundering obligations;
- 62 per cent would refund a double payment immediately – perhaps the easiest way to launder money through a law firm; and
- 25 per cent did not know that they could ask for help if they had a problem on a file.

Sometimes the trigger for a compliance review is an incident, such as a conflict breach. It's important for the review to establish the cause and identify the lessons learned.

“Having compliance procedures and demonstrating compliance are two different things”

Having compliance procedures and demonstrating compliance are two different things. Ideally, file audits will assist in demonstrating compliance. Lawyers may resist this. Some lawyers will spend longer explaining why this cannot be done than it would take them to audit a file!

There can also be logistical challenges, but the process can deliver value even if it does not involve a review of the advice provided, as you can audit the process. A middle course involves an experienced lawyer reviewing the file – a good lawyer will spot issues even if they are not an expert in the particular area under review.

System implementation

The system which you implement to improve your firm's compliance must be proportionate – there is no 'one size fits all' – and it must have regard to what is realistically achievable. Firms should resist the temptation to scrap systems which work. If something works, keep it and, if appropriate, roll it out to other parts of the firm.

Risk registers are in general use in both the corporate and public sectors. In law firms, they are less common, except for in England and Wales, where their use has developed under the regulatory regime in force since 2011, with firms' risk management being under scrutiny by the Solicitors Regulation Authority.

Put simply, a risk register is a list of the firm's risks that evaluates:

- the probability of each risk occurring and the potential impact;
- what steps are being taken to mitigate the risks;
- how to control or transfer risks (or, in some cases, to accept them); and
- who has ownership of each risk.

A risk register does not have to be complex and, while firms can use dedicated software, it can equally be prepared in Microsoft Excel. It should involve input from a cross-section of stakeholders and not be the work of one person alone, or it will only represent that person's perception of risks.

Those best able to understand the risks faced by a practice are those involved in each aspect of it, though they may well benefit from discussion with a third party with a wider overview and knowledge of risk experience in other similar practices.

But, it is important that the risk register does not, metaphorically speaking, sit on a shelf. It should be a living thing – effectively an agenda for the regular review of risks, and updated on a rolling basis.

Getting buy-in is important. Client-imposed requirements can be a significant driver as, without compliance, the work will dry up; this is particularly relevant when it comes to data security.

Increasingly, firms are seeing their management of risk as a competitive advantage. Some are obtaining external accreditation under standards prescribed by the International Standards Organisation, such as ISO 27001 on information security management.

Common issues

Let's now consider some of the common compliance problem areas for law firms.

Supervision

This is probably the area in which the most variance can be seen, even in the same office. Is supervision active? Some lawyers, when asked about their supervision procedures, will say they have an open door policy. This is important, but it is not supervision: it relies on staff knowing they have a problem, and being prepared to ask for help.

“If something works, keep it and, if appropriate, roll it out to other parts of the firm”

As noted earlier, online testing has shown that, even in the best firms, a significant proportion of staff may not feel able to ask for help. If partners do not actively supervise their staff, they are adopting a 'bet the firm' approach with every lawyer, every day.

Client engagement

Client engagement processes become ever more onerous with the increasing imposition of client requirements and developments in the financial crime arena. For all but the smallest firms, centralising the process can make it more effective and more efficient.

“If partners do not actively supervise their staff, they are adopting a ‘bet the firm’ approach with every lawyer, every day”

Most large law firms have gone on this journey, but it is gradually being adopted by smaller firms too. Part of the process is to ensure compliance with key requirements, but also to ensure the work is within the

expertise and resources of the firm and individuals, and that the reward justifies the risk.

Ongoing monitoring

Anti-money laundering legislation in most jurisdictions requires ongoing compliance monitoring in certain circumstances, but it is a consistent area of weakness in the majority of law firms.

Outside counsel guidelines

As noted earlier, these cause significant operational difficulty in relation to conflicts, but also impact on other areas, such as diversity and business continuity.

Information barriers

Are information barriers permitted under your professional rules? Even if they are, can you implement them effectively and will clients be happy with them? Many firms think they can implement them by simply locking down certain electronic files, but proper systems address far wider issues.

Information security

While many firms are focusing on cyber risk, the bigger issues often arise in relation to their people. For example, lawyers have been known to inadvertently breach confidentiality through social media or to take confidential client documents when they leave the firm.

Culture

Would you spot a rogue in your midst? Even the best firms have had them. Would your staff tell someone if they saw a problem? As noted earlier, not all feel able to do so.

Constant review

There is a range of issues to consider when implementing a compliance system. But, like risk management, compliance is a culture, not an event. If your systems are to have any value, they must be kept under constant review and have someone responsible for ensuring that compliance happens.

Reference

1. See 'Reputations at risk', Frank Maher, *Managing Partner*, December 2014/

Frank Maher is a partner at Legal Risk, specialising in professional regulation and professional indemnity (www.legalrisk.co.uk)