Compliance Plan – An Overview

Complacency is not an option when it comes to compliance!

What? Who? How?

What is a Compliance Plan for?

The purpose of a compliance plan is to give an overview of a structure for reviewing and monitoring compliance policies and procedures on a regular basis – to bring some cohesion to the process.

The reviewing and monitoring of compliance within your firm should not be a 'once a year snapshot' of what is going on – it should be undertaken regularly so that there is a genuine understanding of how policies and procedures are working in practice, and how effective they are.

Who is responsible for it?

The responsibility for reviewing and monitoring compliance policies and procedures will mainly fall to the COLP, COFA and MLCO/MLRO. Depending on the size of your firm, there may be more people involved.

Who is the Compliance Plan available to?

The Board? Compliance officers? Everyone? Ultimately, this depends on your firm, its culture, and how the plan will be implemented, used and shared. Some firms may prefer a small group of people to have sight of it and be able to make updates, whilst others may

wish to share it and gather feedback from all staff as to the effectiveness of the policies in practice.

How to implement and use a Compliance Plan?

This document consists of the following components:

1. An overview of what a Compliance Plan should contain and why
2. A (non-exhaustive) list of key policies that a firm should have to successfully manage their compliance obligations (*Appendix 1*)
3. Compliance Review (i.e. what tasks should be undertaken, by whom, throughout a year) (*Appendix 2*)
4. Compliance Plan - Annual Review of Trends and Patterns (i.e. a review of key areas of the Compliance Review with a focus on identifying trends or patterns) (*Appendix 3*)

* This overview provides a focus on compliance plans in the context of the SRA Standards and Regulations.

Background

What are the regulatory requirements about compliance plans?

There is no actual requirement in the SRA Standards and Regulations 2019 for law firms to have a compliance plan - this is in contrast to the expectation in the 2011 regulations where guidance notes stated: *'what needs to be covered by a firm's compliance plan will depend on factors such as the size and nature of the firm, its work and its areas of risk'*.

Individual firms can therefore choose whether to have a compliance plan or not. However, doing so does help the firm to demonstrate that it takes its regulatory obligations seriously. It can also help to provide clarity with other obligations (for example, in relation to governance in the firm, compliance officers and their duties, etc.).

NB. Firms that wish to obtain the Lexcel accreditation, or currently have it, **must** have a risk management policy that includes a compliance plan.

What should be in a compliance plan?

With no requirement to have a plan, firms are free to decide (a) whether to have one, and (b) what it would contain.

For some firms, having everything in one place makes the most sense and is an orderly way of ensuring everyone has easy access. However, for other firms, putting all compliance arrangements in one document may not be overly practical (or possible). In the latter case, it would be feasible for your compliance plan to contain a register of your separate policies and procedures. This would help in keeping the plan simple (see Appendix 1).

Although not required in the 2019 Code for Firms, the SRA did indicate some key areas for consideration in the 2011 regulations. This does provide some helpful guidance if firms are stuck with a blank page – it does not include everything, but is a good start:

1. framework for governance arrangements within the firm
2. compliance officers – who they are and what their duties are
3. accounting procedures
4. a system for ensuring only appropriate people authorise payments from client account
5. a system for giving undertakings
6. checks on new staff or contractors
7. a system for ensuring that basic regulatory deadlines are met
8. a system for monitoring, reviewing, reporting and managing risks
9. procedures for ensuring issues of conduct are given appropriate weight in decisions the firm takes

10. an adequate file review process
11. systems to support / develop / train staff
12. a system for obtaining the necessary SRA approvals
13. a system ensuring duties to clients are fully met during staff absence

A little more on some of these …..

Governance

A regulated firm must have effective governance structures, systems and controls in place that ensure:

1. compliance with SRA regulatory arrangements
2. compliance with other regulatory/legislative requirements
3. compliance of managers and employees with the SRA's regulatory arrangements which apply to them
4. compliance of managers and employees to not cause (or contribute to) a breach of the SRA's regulatory arrangements
5. that compliance officers are able to discharge their duties in accordance with the Code for Firms

A formal, documented compliance plan can help demonstrate your governance arrangements clearly.

Compliance officers – what are they?

It is a requirement that all SRA-regulated law firms must have a COLP (Compliance Officer for Legal Practice) and a COFA (Compliance Officer for Finance and Administration). They can be the same person, or they may be different people (this may depend on the size of the firm).

A compliance plan is the ideal place to state (a) who these individuals are in your firm, and (b) and what they actually do.

What are the duties of the compliance officers?

The (COLP) and (COFA) within the firm must ensure:

1. compliance with the terms and conditions of the firm's authorisation as granted by the SRA
2. compliance by the firm, its managers and employees with SRA regulatory requirements
3. the firm's managers and employees do not cause or contribute to a breach of the SRA's regulatory requirements

The Code for Firms is very clear that managers of the firm have a joint responsibility along with the designated compliance officers for the firm's compliance with the regulatory requirements.

A compliance plan can help to demonstrate how these obligations have been implemented and are actioned by the compliance officers in the day-to-day running of the firm.

What about monitoring and reviewing?

A compliance plan should provide clear guidance on how compliance will be monitored within a firm.

Ideally, every area of compliance would be reviewed on a regular basis to make sure that all policies, procedures and processes are up to date (and that everyone is adhering to them!) However, this is not a practical reality for most law firms.

It may be more practical to review different key areas of compliance on a regular basis. For example, you could have a plan to review the following areas but spread them across a year*:

- file reviews
- compliance failures
- complaints and/or negligence
- risk register
- Firm Wide Risk Assessment (FWRA)
- client care letter
- terms of business
- breach register (including data, accounts, etc.)
- financial stability
- training
- conflicts and confidentiality
- undertakings (if applicable)
- AML and financial crime issues
- data protection and GDPR
- cybercrime, frauds, scams
- referral and fee sharing
- staffing and HR
- website and marketing

** See our free template - Appendix 2 - for how this can be managed.*
Please note - this is not an exhaustive list – this needs to be tailored to the needs of each individual firm.

Reviewing these key areas on a regular basis will provide a good insight into whether a firms' compliance policies and procedures are working as desired.

The COLP has responsibility to:

- keep the compliance calendar as up-to-date as possible

• ensure that the calendar tasks are completed within agreed parameters

The reporting of compliance breaches

The COLP and COFA are required to ensure:

1. a prompt report is made to the SRA of any matters that they believe are capable of amounting to a serious breach of the terms and conditions of the firm's authorisation, Accounts Rules or the SRA's regulatory arrangements which apply to the firm, managers or employees
2. the SRA is informed promptly of any matters they reasonably believe should be brought to its attention in order that it may investigate whether a serious breach of its regulatory arrangements has occurred or otherwise exercise its regulatory powers

What about training?

A compliance plan should make reference to the training of all personnel within a firm – this includes managers/directors and all employees (fee earning and support staff). Everyone needs to be competent to carry out their role, and training is vital to ensure this.

The SRA have a continuing competence requirement for solicitors and RELs whereby they are obliged to ensure they refresh their professional knowledge of the legal profession, subject specific knowledge, ethical knowledge and understanding of their obligations to fulfil their regulatory requirements.

A compliance plan is an ideal way to outline your systems for supporting your staff in their development and training.

Appendix 1

Key Policies

1. Accounts Handling Policy
2. Anti-Bribery and Corruption Policy
3. Anti-Money Laundering and Counter Terrorist Funding Policy
4. Anti-Slavery Policy
5. Breach Reporting Policy
6. Bring Your Own Device (BYOD) Policy
7. Business Continuity Plan
8. Cash Policy
9. Charitable and Political Donations Policy
10. Client Care Policy
11. Complaints Policy
12. Confidentiality Policy
13. Conflicts of Interest Policy
14. Corporate Social Responsibility Policy
15. Coronavirus (COVID-19) Workplace Safety Policy
16. Criminal Records Information Policy
17. Data Protection Policy
18. Data Subject Access Request Policy
19. Email Policy
20. Equality and Diversity Policy
21. File Review Policy
22. Financial Management Policy
23. Financial Sanctions Policy
24. Flexible Working Policy
25. Fraud Prevention Policy
26. Gifts and Hospitality Policy
27. Health and Safety Policy
28. Human Right Policy
29. ICT Policy
30. Induction Policy
31. Information Management and Security Policy
32. Instructing Third Parties Policy
33. Interest Policy
34. Internet Access Policy
35. Introductions to Third Parties Policy
36. Learning and Development Policy
37. Negligence Policy
38. Office of Financial Sanctions Implementation (OFSI) Policy
39. Outsourcing Policy

Sophia House, 28 Cathedral Road, Cardiff CF11 9LJ
(02920) 660160
www.jonathonbray.com

40. Password Policy
41. Performance Management Policy
42. Privacy Policy
43. Publicity Policy
44. Records Management Policy
45. Recruitment, Selection and Progression Policy
46. Referral and Fee Sharing Policy
47. Remote Working Policy
48. Risk Management Policy
49. Social Media Policy
50. Staff Leaving Policy
51. Supervision Policy
52. Trade Sanctions Policy
53. Undertakings Policy
54. Website Management Policy
55. Whistleblowing Policy

Please note - this is not an exhaustive list – this needs to be tailored to the needs of each individual firm.

Appendix 1

Compliance Review

MONTHLY

What to review, when and by whom

What to review	Review in detail	How often	By whom	Notes
File reviews	- Is there a standard system? - Is there a timetable for reviews? - Are reviews shared with fee earners? - Is there a process for ensuring corrective actions are completed? - Is the information shared with the COLP?	Monthly	COLP	
Data protection and GDPR	- **Subject Access Requests** - check any active and see if any patterns to develop into complaints - **Breach reports** - check on any external and any internal. See if any internals form a pattern	Monthly	COLP/DPO	

	which would mean report required to the SRA/ICO - **Data Protection Impact Assessments** – check if active			
Financial Stability	- Has a reconciliation review been done? - Has cashflow been reviewed? - Has the COFA signed off reconciliations? - Have outstanding balances been reviewed?	Monthly	COFA/Partner	

QUARTERLY

What to review, when and by whom

What to review	Review in detail	How often	By whom	Notes
Complaints and/or negligence	- Are there any complaints that need to be responded to? - If relevant, have the insurers been informed? - Have any complaints been resolved? - Does the risk register need to be updated? -	Quarterly	COLP/Partner	
Risk Register	- Review top risks (highest rated). - Does anything new need adding to the register? - Does anything need to be closed off on the register?	Quarterly	COLP/Partner	
Undertakings	- Are there any issues? - Are there any breaches? - Have these been discussed? (at Board Meeting or Partner Meeting or Compliance Meeting)	Quarterly	COLP	
Conflicts and confidentiality	- Have any issues arisen? - How are they dealt with?	Quarterly	COLP	

AML and financial crime issues	- Have there been any Suspicious Activity Reports (SARs) to the MLRO? - Have there been any SARs to the NCA? - How many matters have been rejected due to AML of FC concerns? - Have there been any sanctions reported to the MLRO or to the OFSI?	Quarterly	MLCO/MLRO	
Compliance failures (not including accounts)	- Have there been any minor breaches (non-conformities)? - Have there been any major breaches? - Have they been recorded on the breach register? - Have they been reported to the relevant internal person and/or the SRA?	Quarterly	COLP	
Accounts rules breaches	- Have there been any minor breaches (non-conformities)? - Have there been any major breaches? - Have they been recorded on the breach register? - Have they been reported to the relevant internal person and/or the SRA?	Quarterly	COFA	
Cybercrime, frauds, scams	- Has the firm caught any? - Has the firm fallen for any?	Quarterly	COLP/MLRO	
Referrals and fee sharing	- Have there been any changes? - Are all the agreements up to date?	Quarterly	COLP	

	- Is the documentation to clients up to date?			
Data Protection and GDPR	- **Data Protection Impact Assessments** – check to see if there are any planned changes to the way data (especially personal) is handled including new technology, and whether there needs to be a DPIA or a change to the Data Protection/Privacy Notice	Quarterly	COLP/DPO	

ANNUALLY

What to review, when and by whom

What to review	Review in detail	How often	By whom	Notes
Website and marketing	- **Website Review** – has the website been reviewed to ensure compliance with the Transparency Rules? - **Marketing** – are all marketing materials compliant with SRA guidelines?	Annually	COLP/Partner	
Client Care Letter	- Have there been any changes? - Is it up to date and accurate?	Annually	COLP	
Terms of Business	- Have there been any changes? - Is it up to date and accurate?	Annually	COLP	
FWRA	- **Full Review** to include any high risk matters in the year, update to any changes on how business is conducted, recorded audit trail of how review has been completed, etc.	Annually	COLP/Partner	
Staffing and HR	- Is the website up to date and an accurate reflection of staff?	Annually	COLP/Partner	

	- Have you conducted ongoing vetting of staff? (e.g. DBS checks as appropriate, references for new staff, practicing certificates for all staff, annual appraisals for all staff). - Review register of interests?			
Training	- Ensure fee earners have completed their Continuing Competence. - Ensure all staff have completed key compliance training.	Annually	COLP/Partner	
Data protection and GDPR	- **Data destruction** - ensure paper and electronic records are being destroyed as per the retention period. - **ICO registration.**	Annually	COLP/DPO	
Financial Stability	- Have any residual balances been paid to charity in line with the firms' policy?	Annually	COFA/Partner	

** This is not an exhaustive list – this needs to be tailored to the needs of each individual firm.*

Appendix 3

Compliance Plan

Annual Review of Trends and Patterns

It is considered good practice to review key areas of your firms' compliance on an annual basis to specifically look out for trends or patterns that may emerge. Whilst you may be monitoring such areas more regularly (e.g. monthly), it can be more difficult to spot trends and patterns in a shorter timeframe.
Reviewing these holistically on an annual basis can help in identifying things that might otherwise slip under the radar.
When is the best time to do this? There is no right or wrong time. However, a good point of reference may be before the firms' insurance renewal is due as it could assist in the preparation for the renewal, as well as helping to ensure appropriate cover is in in place.

Review area	**Is there a pattern? (Y/N)**	**If there is a pattern:**				**Further notes** **Review conducted by?** **Date?** **Further action?**
		Does it form a reportable breach? *(provide details)*	**Has the risk register been updated?** *(provide details)*	**Has the firm policy been updated?** *(provide details)*	**Have staff received sufficient updated training?** *(provide details)*	
File reviews						
Complaints and negligence						
Undertakings						
Conflicts and confidentiality						
Compliance failures						

Accounts rules breaches						
Cybercrime, frauds, scams						

** This is not an exhaustive list – this needs to be tailored to the needs of each individual firm.*