Practice Assurance guidance for larger firms

STANDARD 4: QUALITY CONTROL

Your firm should ensure that work is conducted in an environment where quality is monitored. A firm should have procedures and systems in place, appropriate to its size, to ensure that:

- the work of the firm is organised and controlled to ensure Practice Assurance standards are met;
- appropriate supervision and review arrangements are applied;
- all work undertaken is adequately recorded;
- all principals and staff are made aware of the firm's systems and procedures;
- the firm complies with its own procedures; and
- any complaints from clients are dealt with promptly and effectively

Guidance

Much of the guidance we have issued to sole practitioners and smaller firms also applies to larger firms. You can access that guidance here.

Strong quality control policies and procedures are a good way to manage risk in any practice. It is important that principals and staff follow these policies and procedures and that firms monitor compliance with them. This is particularly important for larger firms that have many staff of varying levels of competence and experience, sometimes over several locations.

Set out below are some top tips, essentials and areas of best practice on how larger firms can comply with some laws, regulations and standards.

Top tips to help you comply

Organisation and control

- Make sure relevant policies and procedures are readily available to principals and staff.
- Train staff in the application of policies and procedures.
- Have regular meetings to plan and manage WIP and deadline management.
- Put someone senior in the firm in charge of destruction of files/documents/information to help ensure this happens in accordance with the firm's policy.

IT procedures and security

- Have a system in place to make sure all principals and staff have read the firm's IT policies and procedures – this could be monitored electronically.
- Give guidance and training on the application of new IT policies and procedures.

- Follow up findings from any IT audit with additional training, updates to procedures and/or software as appropriate.
- Obtain ISO27001 certification on your information security management system.
- Obtain Cyber Essentials certification to help protect your firm against cyber-attack.

Supervision and review

- Make it clear to staff and principals why a review is required.
- Have review requirements embedded into your procedures.
- Ensure your procedures flag the requirement for a review early so you can plan sufficient time for the review to be undertaken.

Recording work

- Ensure any guidance and training has made it clear to principals and staff what and how much they need to record.
- Build in validation checks to some procedures to highlight areas that have not been recorded sufficiently.
- Ensure any cold file reviews include consideration of the adequacy of recording work.
- Make sure you use reviewers with the right level of expertise and authority so they identify issues and have the credibility to challenge.

Complaints from clients

- Conduct customer satisfaction surveys to help identify areas for improvement at an early stage.
- Train staff to recognise early signs of client dissatisfaction.

Compliance review

- Ensure reviewers are trained so they understand the purpose of the reviews and what is expected of them.
- Reviewers need to be sufficiently independent so that they do not review their own work or that of their close colleagues.
- Read the results of our review, Practice Assurance reviews – large firms.

Best practice

Organisation and control

- Develop and maintain a risk register for your firm to enable you to mitigate and monitor the risks to the practice.
- Documented standard procedures in place for all types of work.
- Ensure the same procedures are followed in all offices.
- Provide clear guidance on the application of policies and procedures.
- Put systems in place to manage WIP and deadlines.
- Have a documented file/document/information destruction policy.

IT procedures and security

- Make sure written procedures are in place for use on all IT systems across the firm to include email and internet usage, use of mobile devices and ‘bring your own’ devices.

- Carry out regular audits of IT systems and procedures to ensure they are up-to-date, have the appropriate licences and are being used in accordance with the firm's written procedures.
- Carry out regular penetration testing to see if the systems are secure.

Supervision and review

- Make sure your firm has clear lines of supervision and policies for when work needs to be reviewed.
- Document reviews so it is clear what has been reviewed and who reviewed it.
- Identify risks within your business that would drive a review requirement eg, complex work, ethical issues, industry type, high profile client and staff competency/experience.

Recording work

- Use standard programmes for each type of work the firm does to help structure and record the work.
- Ensure systems and procedures are such that principals and staff can record all their work, judgements, conclusions and reviews. This should include who did the work and when it was done.
- Make sure key conversations and meetings with clients are documented and that key instructions from clients are received in writing (email is fine).

Trust work

See also the results of our focused review in this area in Practice Assurance Principles 2018.

- Make sure you have a policy for which individuals in the firm can take on trustee and executor appointments.
- Maintain a central register of trusteeships, executorships and powers of attorney.
- Have standard procedures, including a filing structure for correspondence and documents for trust work.

Complaints from clients

- Consider collecting positive feedback at the same time as any indication of complaints.

Compliance review

- Conduct cold file reviews on non-audit assignments.
- Ensure all areas of the firm are covered over a period of years but flex to take account of known risk areas.
- Make sure file reviews cover compliance with procedures and technical content.
- Make sure whole-firm risks are covered including any input from clients such as customer satisfaction surveys and/or complaints.
- Prepare action plans to address issues identified in reviews and monitor the progress of those plans.