Practice Assurance guidance for larger firms

STANDARD 1: LAWS, REGULATIONS AND PROFESSIONAL STANDARDS

Your firm should comply with laws, regulations and standards that are relevant to the services it provides, including ICAEW's regulations, standards and guidance.

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.

Larger firms have more staff and in general, offer more services. This means that a wide range of laws, regulations and standards are likely to be relevant to the firm. So it's important that someone in your firm has sufficient knowledge of your whole business to recognise what laws, regulations and standards apply.

Laws, regulations and standards change, so your firm needs to have robust mechanisms in place to identify changes and consider their impact. You then need to put in place or update policies procedures and guidance to address the changes. Most importantly, your firm needs to ensure staff understand them and the impact of any updated policies and procedures.

Set out below are some top tips, essentials and areas of best practice to help larger firms comply with some of the laws, regulations and standards.

Top tips to help you comply

Anti-money laundering (AML)

- Use a central team/resource to help engagement teams complete AML procedures.
- Record and save AML client due diligence (CDD) on a central electronic system. This can allow you to set flags for when CDD needs refreshing and allows monitoring through exception reporting.
- Set renewal dates for refreshing AML CDD and lock clients' accounts if they are not updated in time.
- Deliver frequent, varied AML training to maintain awareness and improve understanding. Frequent short training sessions on narrow AML issues are often more effective than comprehensive, less frequent training.
- Use our AML guidance to help you comply with the ML17 requirements.

Clients' money

- Administer and control clients' money centrally rather than in different offices.
- Designate a senior member of management as being responsible for clients' money.
- Make sure your annual clients' money review covers all the Clients' Money Regulations. Our helpsheet can help you with these reviews.

Data protection and security

- Access ICAEW GDPR guidance.
- Access ICO GDPR guidance.
- Consider obtaining ISO27001 accreditation.
- Use the Cyber Essentials resources and get certification to help protect your firm against cyber-attack.
- Have an external review of your data protection processes and procedures.
- If you use third parties to outsource work and/or data storage, it's a good idea to visit them periodically and conduct your own review of their policies and practices.

Tax

- Deliver training to relevant staff on the content and application of professional conduct in relation to tax (PCRT). This could include example scenarios on how PCRT is likely to affect day-to-day work.

Other laws, regulations and professional standards

- If you describe a member of staff as a partner or director to clients and third parties, make sure it is clear that the staff member is not a principal in the firm to avoid them holding out as such.
- Make sure you consider the impact any changes to the structure of your firm or group may have on your eligibility for member firm status, use of description Chartered Accountant, audit registration, DPB licence, probate accreditation, licenced practitioner registration and use of consumer credit arrangements.
- If you don't have a DPB licence and are not FCA registered make sure you are familiar with what activities are regulated and require a licence or registration. Consult our DPB (Investment Business) Handbook for more information.
- Be aware of what element of probate services are regulated legal activities which require the firm to have probate accreditation. For more information see our regulatory advisory on when to seek a probate licence.

Essentials

Anti-money laundering (AML)

- Make sure you have updated your AML policies and procedures for the key changes brought in by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR17).
- You must conduct a whole-firm risk assessment.
- Make sure you have procedures in place across all service lines (payroll-only is one of the main areas firms miss).
- Make sure you retain AML CDD documentation for at least five years after the client relationship ends.
- Make sure you conduct and document an AML risk assessment for long-standing clients.

- If your firm or a connected entity is not an ICAEW member firm, ICAEW is not automatically your money laundering supervisor and you may need a contract.

Clients' money

- Only handle clients' money if it relates to an accountancy service being provided to the client – be aware of clients' money regulation 8A.
- Make sure AML CDD is conducted when clients' money is received from a client for the first time.

Data protection and security

- Make sure all relevant entities connected to the firm are registered with the Information Commissioners Office.

Best practice

Anti-money laundering

- Make sure your AML procedures are well documented, clear and cover all types of client.
- Back-up your procedures with comprehensive tailored guidance and training.
- Use similar or the same AML procedures across all service lines.
- If you use an electronic checking system as part of your CDD procedures make sure you know what it is checking against and that staff are trained to interpret the results.

Clients' money

- Have clear written clients' money procedures that are made available to everyone in the firm. These should define what clients' money is and under what circumstances the firm will handle it. It should include guidance on the application of clients' money regulation 8A.
- Donate clients' money that has gone unclaimed for five years or more to charity.

Data protection and security

- Make sure you have put in place changes to address the requirements of the General Data Protection Regulation (enforcement date of 25 May 2018).
- Encrypt all USB sticks and laptops.
- Use a client portal to transfer and exchange information.
- Deliver regular staff awareness campaigns and training.
- Monitor email and IT activity.
- Develop policies and procedures around BYOD (bring your own device).
- Procure reviews and assistance from outside consultants to conduct penetration testing or resilience testing.
- Have formal procedures in place to report a data loss or security breach.
- If you outsource work or data storage to a third party ensure you have data confidentiality and storage clauses in your contract, and that your suppliers' data protection policies and procedures are appropriate and up to date and comply with EEA requirements.
- Periodically review your policies, procedures, guidance and training.
- If an assignment requires Chinese Walls make sure they are fully secure with strict access controls.

Tax

- Have procedures in place to both identify and deal with clients (both new and existing) to whom the Foreign Account Tax Compliance Act (FATCA) applies.
- Have procedures in place to both identify and deal with clients (both new and existing) to whom the Common Reporting Standard applies.
- Have procedures in place to identify and deal with trusts that need to register with HMRC.