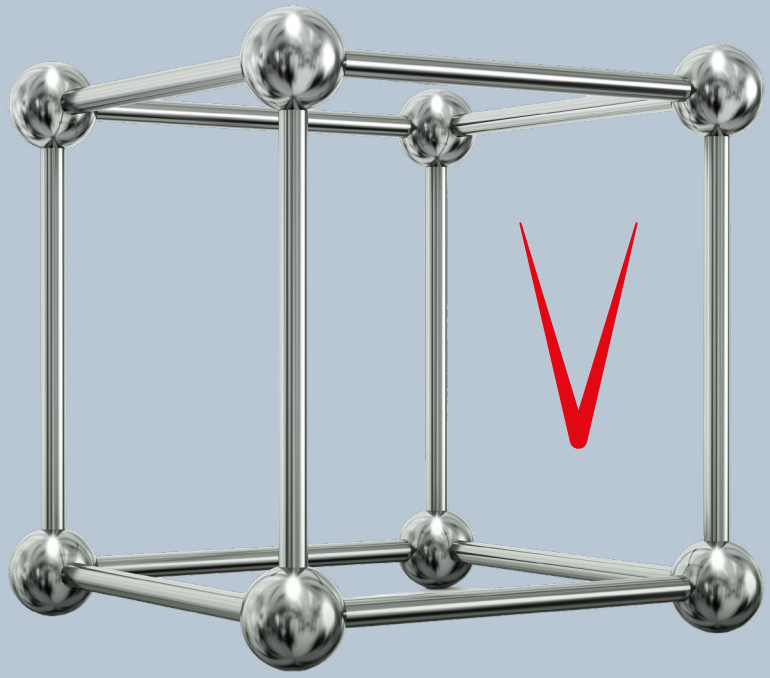


A FRAMEWORK FOR GOOD PRACTICE

PRACTICE ASSURANCE MONITORING REPORT 2026

icaew.com/regulation

PROFESSIONAL STANDARDS DEPARTMENT

ICAEW – PRACTICE ASSURANCE MONITORING

Who we are and what we do

Our approach is to work as an improvement regulator, helping members and firms maintain high professional standards and holding them to those standards.

A broader overview of our regulatory work is available in the ICAEW Regulation and Conduct Annual Report: Trust through accountability

Independent decision-making

ICAEW's governance structure ensures its regulatory and conduct roles are not influenced by its representative functions. View Appendix 1 for more information about the oversight and governance of ICAEW's regulation and conduct activity.

Contents

1 Who we are and what we do
2 About the Practice Assurance scheme and its benefits
3 Monitoring review outcomes
10 2025 area of focus: cyber security
16 2026 areas of focus
17 Feedback from firms
18 Help and support from ICAEW
19 Appendix

About the Practice Assurance scheme and its benefits

The Practice Assurance scheme has been a cornerstone of ICAEW's quality assurance framework since 2004. It provides assurance that ICAEW practising certificate holders, member firms and firms with a contract for Practice Assurance operate in accordance with professional standards, ethical requirements and relevant regulations.

For their clients, it provides reassurance that they're working with a regulated firm committed to high standards with independent oversight, clear ethical requirements and safeguards that are in place to protect them and the wider public interest.

ICAEW's Practice Assurance monitoring activity

ICAEW undertakes a wide-ranging programme of monitoring to assess firms' compliance with the Practice Assurance framework.

We aim to review all firms at least once every eight years. We may select firms for a review more frequently, depending on risk factors such as:

- the size and complexity of the firm;
- previous review history; and/or
- factors identified from our risk monitoring activities.

This report shares the findings from more than 2,000 Practice Assurance monitoring reviews carried out by ICAEW's Quality Assurance Department during 2025.

At 88% of firms, we either raised no matters requiring action or the firm addressed the matters we raised with no need for follow up.

We reflect on the most common issues identified during our monitoring activity, many of which are recurring themes from previous years. We therefore recommend that firms read this report (and the pitfalls it highlights) carefully to avoid making similar mistakes.

Each year, we hold detailed discussions with larger firms to explore selected areas of focus in more depth. These conversations include a review of the policies and procedures firms have in place to manage risks in relation to these topics. Our area of focus for 2025 was cyber security and the details of our findings can be found on page 10 of this report.

Webinar and CPD opportunity

Register for our free 2026 Practice Assurance Monitoring Results webinar, which explores the findings of this report, including the results of our focus on cyber security.

5 June 2026 | Register now or if you missed it, tune into the recording.

2,000+
Practice Assurance monitoring reviews

At 88% of firms, we either raised no matters requiring action or the firm addressed the matters we raised with no need for follow up.

Dean Neaves
ICAEW Senior Manager, Quality Assurance

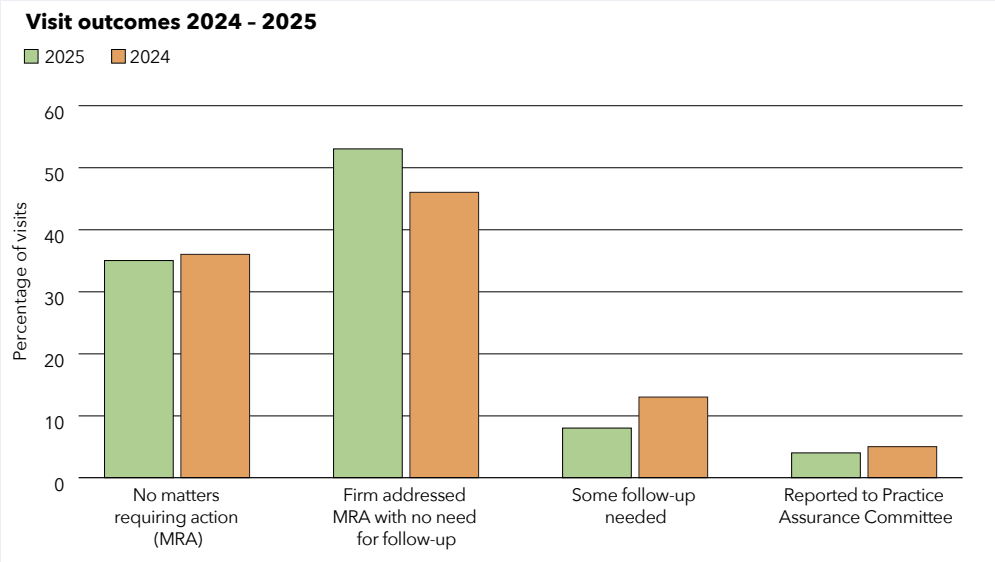
"We hope all the findings we have shared in this report help your firm reflect on its policies and procedures, identify areas for improvement and take inspiration from what other firms are doing well."

Monitoring review outcomes

The table opposite is a summary of the results from Practice Assurance monitoring reviews carried out by ICAEW's Quality Assurance Department in 2025.

Some of our reviews cover more than one firm, where there are several entities connected by virtue of direct or indirect common principals, ownership, control or management. In 2025 we carried out 1,715 separate Practice Assurance reviews covering 2,068 firms (2024: 1,185 reviews covering 1,489 firms).

Delivery method	No matters requiring action (MRA)		Firm addressed MRA with no need for follow-up		Some follow-up needed		Reported to Practice Assurance Committee		Number of firms	
	2025	2024	2025	2024	2025	2024	2025	2024	2025	2024
On site	16%	13%	65%	58%	11%	21%	8%	8%	819	691
Desk-based reviews, including new firm reviews	99%	99%	1%	1%	–	–	–	–	422	345
Telephone reviews	21%	23%	67%	63%	9%	10%	3%	4%	827	453



Monitoring review outcomes continued

In 2025, the Practice Assurance Committee considered 81 visit reports (2024: 45 reports). Some of the reasons for these reports are listed below.

- 34 firms had significant weaknesses in complying with the Money Laundering Regulations, with some failing to fulfil assurances provided at the previous review to improve their procedures. In some cases, they also failed to fully comply with Clients' Money Regulations.
- 28 firms were using the description 'Chartered Accountants' when they were not eligible to do so.
- 19 firms had significant breaches of Clients' Money Regulations.
- 4 firms had significant gaps in their professional indemnity insurance (PII).
- 6 firms had not notified clients of commission received or obtained consent to retain it.

The Practice Assurance Committee also considered 11 other reports for matters including failure to provide requested information following a previous visit and instances of non-compliance with previous decisions made by the committee.

The Practice Assurance Committee issued penalties of up to £10,000 to 44 firms (2024: 25 firms), and 37 (2024: 23) were referred to ICAEW's Conduct Department for further investigation.

HINTS AND TIPS

Review the points raised at your last Practice Assurance review and ensure you have taken action to address all the issues. **Failure to address issues raised at the previous review is a common reason for firms being reported to the Practice Assurance Committee.**

If your firm is using the description 'Chartered Accountants', check that you are eligible to do so by reviewing the ICAEW guide: Use of the description

Use the wide range of helpful resources available for AML-supervised firms on the ICAEW website to help ensure that you are fully compliant with the Money Laundering Regulations

If you hold clients' money, ensure that you are familiar with the Clients' Money Regulations and have robust procedures to comply with them.

View our Practice Assurance compliance review helpsheet

Monitoring review outcomes continued

Analysis of findings

The table opposite shows instances of reviews with firms that have at least one finding that relates to non-compliance with regulations. The list is similar to last year and we therefore recommend firms review it carefully, alongside the relevant regulations and the resources identified below, to ensure they are not making similar mistakes.

Finding	No. of breaches	% reviews/ visits	2025 ranking	2024 ranking
Money Laundering Regulations	937	63%	1	1
Basis of fees and complaints, and engagement letters	283	19%	2	3
ICAEW records and annual return	252	17%	3	4
Clients' Money Regulations	241	16%	4	2
Referrals and commissions	158	11%	5	5
Professional indemnity insurance	125	8%	6	7
Eligibility	90	6%	7	6
DPB (Investment Business) and/or probate boundary issues	77	5%	8	9
Objectivity and other Code of Ethics findings	12	1%	9	10
Other isolated findings including data protection	35	3%	10	N/A

Please note that more than one area of non-compliance may apply to a single firm, so the numbers overlap.

Monitoring review outcomes continued

Most common findings

Alongside each finding, with the number of firms in our sample where we found issues, we have listed examples of ICAEW resources or other guidance that we recommend firms use to improve compliance in these areas.

Money Laundering Regulations
We publish an annual report on anti-money laundering (AML) which explains the findings from our monitoring reviews together with information on our regulatory role and how we fulfil it. We recommend reading the report for a breakdown of AML compliance issues and relevant available resources.

Relevant resources
AML supervision report
AMLbites
AML resources

Basis of fees and complaints, and engagement letters
In 2025, 273 firms had not informed their clients of:
- the basis on which fees are charged; and/or
- the firm's complaints procedure, including the client's right to complain to ICAEW.

You do not have to issue engagement letters to clients, but the above two matters must be communicated to all clients in writing.

If you don't want to issue an engagement letter, you could communicate these matters to clients in any of the following ways:
- a standard "terms of business" letter;
- a brochure given to the client; or
- a paragraph in the body of the initial correspondence.

We also found issues where firms were not keeping their engagement letters up to date, did not cover specialist services and/or were incorrectly informing clients that they were able to carry out work requiring a DPB (Investment Business) licence when this was not the case.

ICAEW has issued updated engagement letter templates incorporating several significant new schedules designed to reflect recent regulatory, operational and technological developments.

Relevant resources
Engagement letters
ICAEW issues Engagement Letter updates: Key changes and guidance for firms

Eligibility issues, ICAEW records, notifying ICAEW of changes and annual return
Finding errors in firms' annual return data and/or ICAEW records is the third highest area of concern.

When completing your firm's annual return, please be careful and check all standing data. If you find an error let us know what we need to do to correct it.

You should take care to ensure you complete your annual return form correctly. If you are unsure about how to answer any question, you should consult the guidance notes and/or call our annual returns helpline +44 (0)1908 546 372.

Importantly, you must notify us of any changes to the structure of your firm within 10 business days. Don't use the annual return for this purpose as you will be in breach of the Practice Assurance Regulations.

How to notify us
1) For firms working in the specialist areas of audit, ATOL reporting, DPB (Investment Business) and the reserved legal services of probate, estate administration and oaths administration - use your standing data change forms to tell us about changes to principals, offices, trading names, ownership structure and regulatory contacts. Completed forms should be emailed to regulatory.support@icaew.com
2) For firms not working in these specialist areas - please tell our members' information team about any changes to your firm structure in writing, by post or email firms.admin@icaew.com

> Access full details of how to notify us of changes, including forms and contact details

Monitoring review outcomes continued

Check carefully whether any changes to your firm's structure have impacted on your firm's eligibility, and whether your firm:

- can use the term 'Chartered Accountant';
- is a member firm under the Practice Assurance Regulations and therefore automatically supervised by ICAEW for money laundering; or
- needs to check other eligibility matters.

Relevant resources

Your guide to maintaining your firm's record

Use of the description 'Chartered Accountants'

Eligibility considerations

Regulated firm restructures and reorganisations

Annual return to ICAEW guidance notes and FAQs

Clients' Money Regulations

Non-compliance with the Clients' Money Regulations remains one of the top areas of concern. We identified that:

- 109 firms did not have a bank trust letter to acknowledge the status of clients' money bank accounts;
- 63 firms had not carried out and documented an adequate annual clients' money compliance review;
- 47 firms were not using designated clients' money accounts when holding £10,000+ for more than 30 days;
- 41 firms were handling or holding clients' money which was not related to accountancy services being provided;
- 33 firms had not obtained their clients' consent, or waited for at least 30 days after issuing an invoice, before taking their fee from a client money balance; and
- 26 firms had not reconciled their clients' money accounts at least once every five weeks.

These are all breaches of the Clients' Money Regulations – firms should regularly review their procedures to ensure full compliance.

Relevant resources

Clients' Money Regulations helpsheet

Clients' money FAQs

Clients' Money Regulations compliance review checklist

Code of Ethics, referral fees and commissions

We identified gaps in accounting for unregulated commissions and/or referral fees at 158 firms. Typically, this is where firms have not told their clients in writing how much they received and/or obtained their consent to retain it.

The ICAEW Code of Ethics 2025, section 330, sets out your requirements to:

- notify all relevant clients in writing of the amounts you have received;
- obtain their written consent to retain it; and
- treat the amounts received as clients' money and bank them in a client account until you have permission to retain the money.

For unregulated activities, you can obtain advanced informed consent by including an appropriate paragraph in your engagement letter that includes examples of likely commissions and amounts. However, you will still need to tell the client the amount once received.

Relevant resources

Engagement letters and privacy notices

ICAEW Code of Ethics

Introductions to financial advisers

Monitoring review outcomes continued

Professional indemnity insurance (PII)
The main findings in this area related to firms being inadequately insured and/or having a policy that did not comply with the ICAEW PII Regulations. You need to make sure your firm's PII meets ICAEW's minimum requirements.

There were also a number of findings relating to notifications not being made to the insurers and errors on proposal forms. Both could result in problems should a claim arise.

ICAEW issued revised PII Regulations in 2024, which took effect from 1 September 2024. Check you are up to date with these requirements, which state the following.

- The policy needs to be with a participating insurer who has agreed to meet the requirements of ICAEW's minimum policy wording. The minimum limit of indemnity is £2m for any single claim and in the aggregate.
- For firms with a gross fee income which is below £800,000, the minimum requirement is two-and-a-half times the firm's gross fee income, subject to a minimum of £250,000 per claim and in the aggregate.
- Larger firms with gross fee income over £50m are not required to put in place 'qualifying insurance' but must have in place appropriate arrangements which will be monitored.
- For firms that are required to put qualifying insurance in place, the maximum aggregate excess should not exceed the higher of £3,000 or 3% of a firm's gross fee income.

Relevant resources

PII information and ICAEW's list of participating insurers

PII requirements: What changed on 1 September 2024?

What to do if you have any issues obtaining PII

DPB (Investment Business) boundary issues and referrals to financial advisers
It's important to review the requirements outlined in the ICAEW Code of Ethics, section R331.17 when considering making referrals to financial advisers. We identified issues relating to referrals to restricted advisers, or where the adviser status was not known, at 92 firms.

Clients rely on you for objective advice, so you should only refer to financial advisers who are able to give sufficiently objective advice. This means you need to know whether your chosen financial adviser is independent or restricted by the Financial Conduct Authority (FCA). You should ensure that the client's requirements can be met by an adviser who can advise across a market that comprises all retail investments that are capable of meeting the needs and objectives of that client.

To make a referral to a restricted adviser you need to ensure that your client's needs will be addressed appropriately by making an assessment of whether the restricted adviser places business with product providers who account for a large majority of the relevant market, or offer the sector of the market which is most suitable for your client's needs.

If you are not confident that you have the knowledge to make this assessment, you should only refer to independent financial advisers.

You should also be aware that some types of referral to financial advisers may require a DPB (Investment Business) licence.

RQ is a referral-management platform, developed in partnership with ICAEW, that helps accountancy firms ensure compliance by managing and tracking referrals. It ensures compliance when referring and generating referral data. ICAEW members have free access to the core functionality of RQ.

Relevant resources

ICAEW Traffic Light Guide to Investment Business Activity

Introductions to financial advisers and other DPB (Investment Business) webinars

Referrals to financial advisers: staying compliant article

ICAEW Code of Ethics, section R331.17

Referral compliance tool (RQ)

Probate boundary issues
Probate and estate administration are closely aligned activities. ICAEW members and firms may carry out the latter as part of their practice and from October 2025, accredited probate firms are also authorised to offer oaths administration. Probate is a reserved activity that requires authorisation or a licence from an approved regulator (AR) or licensing authority (LA). ICAEW was designated as an AR and LA in 2014.

Monitoring review outcomes continued

Where a member or member firm engages in estate administration services (be it as executor or acting for the executor) and also undertakes probate-related activities which are managed as a process, and a fee is involved, then the practitioner should be licensed for the reserved service.

Relevant resources

Probate resources

Regulatory advice on when to seek a licence for probate

Objectivity

We don't identify too many issues in this area. The findings tend to be specific to individual clients, so it is difficult to highlight particular themes.

Threats to objectivity may result from having interests in, or relationships with, a client or their directors, officers or employees. It is best to consider these matters before undertaking any new work and during the course of an appointment, as threats can arise at any time.

Threats to objectivity may be:

- actual – are there relationships that are so significant that they could tilt the firm's judgement away from that which would be the professionally objective, right thing to do? or
- perceived – are the relationships such that a reasonable and informed third party would consider that objectivity would be impaired?

When evaluating the significance of the threats, firms should consider both the nature of the service provided and the nature of the relationship.

Where safeguards are considered necessary, examples might include:

- changing the personnel on the engagement team where the firm has staff (eg, using staff who do not have significant personal relationships with the client);
- discussing the matter with the board or other affected parties;
- disclosing the relationship to affected parties; and
- undertaking reviews (internal or external) of the work performed.

ICAEW members, affiliates, ICAEW students and staff in firms with member firm access can discuss their specific situation with the Ethics Advisory Service on +44 (0)1908 248 250.

The 2025 edition of the ICAEW Code of Ethics came into effect on 1 July 2025. Key changes relate to:

- the role and mindset expected of professional accountants;
- the impact of technology; and
- professional and personal conduct.

Relevant resources

ICAEW Code of Ethics 2025

The role and mindset expected of professional accountants

Data protection

The main finding in this area related to five firms that had not registered with the Information Commissioner's Office (ICO).

Relevant resources

Information Commissioner's Office registration

UK GDPR guidance and resources

ICAEW data protection and privacy guidance

2025 area of focus: cyber security

We discussed cyber security with 121 larger firms during our 2025 monitoring activity. All of the percentages within this section refer to the percentage of respondents from the firms we spoke to on the topic of cyber security.

Awareness and impact

- 99% of firms felt they had a good level of awareness of cyber security threats and had robust procedures and controls in place to prevent and/or respond to attacks. A similar proportion felt that the threat of cyber security breaches/attacks is leading to fundamental operational changes to the way they work.
- 99% were aware of the Cyber Essentials certification scheme in the UK.

"We believe we have appropriate procedures in place to stop any threats to IT security, but the threat is always very high."

An ICAEW firm

- 54% had completed the Cyber Essentials basic self-assessment questionnaire, to assess and demonstrate how their key security controls meet the scheme's requirements.
- 29% completed Cyber Essentials Plus (additional on-site testing by external certifying bodies).
- 38% were aware of ICAEW's cyber security resource centre web pages.
- 15% are certified under either the ISO27001 Information Security Standard (an international standard that specifies the requirements for establishing, implementing, maintaining and improving an Information Security Management System) or the Information Assurance for Small and Medium Enterprises (IASME) Cyber Assurance Standard (a cyber security certification framework designed to help SMEs protect their digital assets).

"Cyber threats are growing at an exponential rate globally. Disruptive technology, such as generative AI, IoT (internet of things), 5G, the metaverse and quantum computing, is being introduced into an environment shaped by complex supply chains, hacktivism and ransomware."

An ICAEW firm

Risk management

In the previous 12 months, 88% of firms (or their third-party IT providers) had used specific tools for security monitoring, 67% had performed risk assessments covering cyber security risks and 62% carried out a cyber vulnerability audit using either internal or third-party IT specialists or consultants.

Of those firms where audits were performed, 52% were carried out either annually or every six months. Some were more frequent; others less frequent or on an ad hoc basis.

51% of firms had carried out penetration testing and 58% invested in threat intelligence, such as active tracking and dark web monitoring on key words and/or subscriptions to threat intelligence products and services.

Only 45% included cyber security risks in their organisational risk register.

"Payroll provides an additional threat given the level of information held within the systems, although we treat all areas with the same high standards."

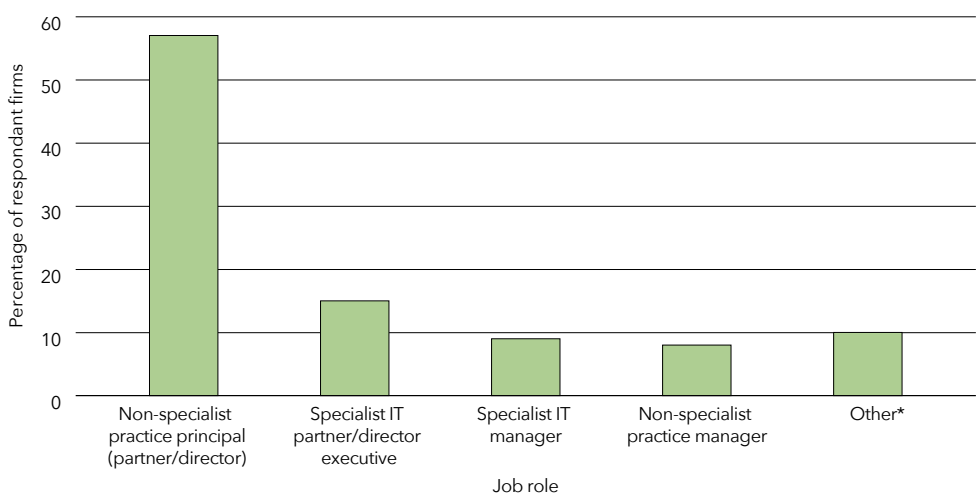
An ICAEW firm

2025 area of focus: cyber security continued

Engagement and training

At the majority of firms (57%) overall responsibility for cyber security was taken by a non-specialist practice principal. Specialist IT managers or directors held the responsibility at 26% of firms.

Overall responsibility for cyber security



*includes other arrangements specific to firm's structure, including group arrangements.

72% had a designated information security officer or equivalent.

90% provided guidance to staff on cyber security matters, including an explanation of cyber security, a description of the firm's policies for prevention and detection of cyber security breaches and guidance of what to do in the event of an actual or attempted attack.

Firms' cyber security guidance is shared within a staff handbook, via policies and procedures published on the firm's intranet and through less formal guidance delivered within email or verbal updates.

82% train staff on good cyber practices and awareness of common attack methods such as phishing and social engineering. Training is delivered through methods including regular, formal training courses, and less formal methods such as through discussion.

Awareness is tested by dummy phishing attacks, quizzes, completion of training assessments and further training provided if responses are unsatisfactory.

"While measures are in place to manage security risks, we recognise that formalising policies and procedures could further strengthen our approach, and this is something that we plan to consider as part of our ongoing cyber security improvements."

An ICAEW firm

2025 area of focus: cyber security continued

Asset management

86% of firms kept a list of critical assets such as data, software, devices and infrastructure. For those deemed critical, 81% had contingency or business continuity planning in case of outages or breaches.

A majority of firms had policies and procedures for managing the security risks of home working (88%), web applications (83%), employees using their own devices (81%) and wireless devices (79%).

Architecture and configuration

80% of firms held critical systems and data on either the cloud or a hybrid of cloud and on-site servers.

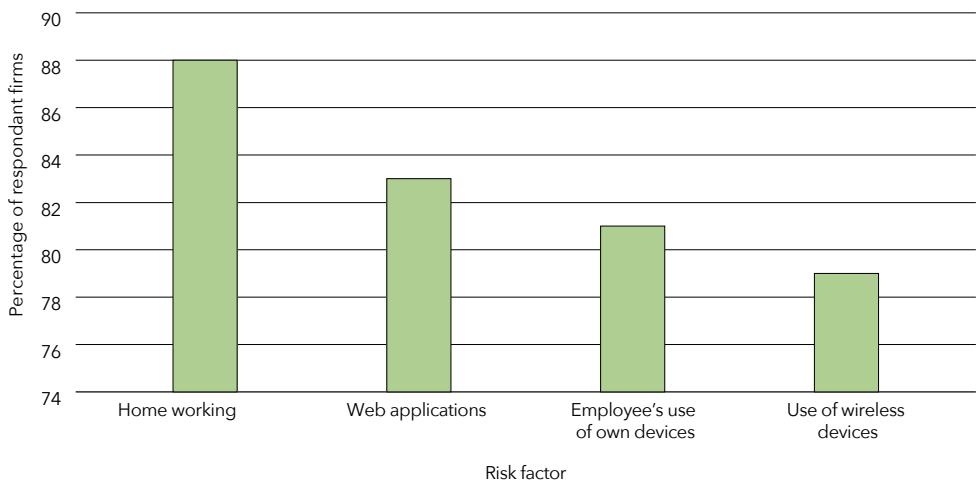
Decisions on selection of system hosting were driven by factors such as advice from external IT consultants, sharing of information, data security, cost and resilience.

82% only permit access to organisation systems through organisational devices and 89% provide separate Wi-Fi networks for guests and employees. 79% use a VPN (virtual private network) and 89% have rules in place for personal data storage and transfer using their systems.

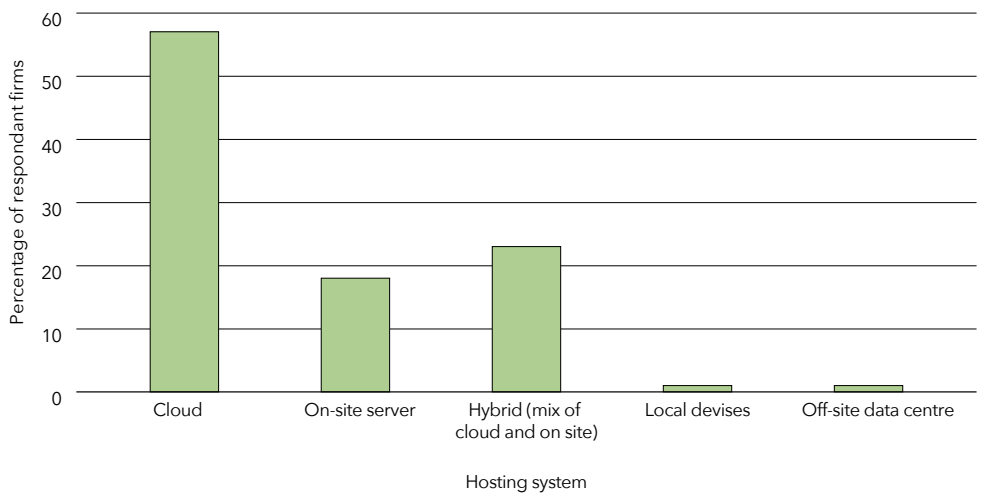
"The cloud solution opted for provides the necessary infrastructure, configurations, security, user management, access controls, redundancy and compliance without the complexities of hosting and maintaining it within the office."

An ICAEW firm

Policies for managing security risks



Data hosting system



2025 area of focus: cyber security continued

Vulnerability management

99% of firms ensure that their systems are always up to date with the latest security patches and 69% ensure that critical systems are segregated from other systems.

"Windows updates and security and critical updates occur weekly. Enforced patches have to happen."

An ICAEW firm

"Cyber Essentials accreditation requires the firm to remain up to date in this area."

An ICAEW firm

Identity and access management

91% of firms have minimum password length complexity requirements and 88% require two-factor or multi-factor authentication for a device trying to access the organisation's network.

Policy on frequency of password changes varies from no specific requirements to periods ranging from 30 to 180 days. There were mixed views on the merits of frequent password changes with some firms considering it leads to weaker passwords.

Other controls on work-issued devices include: device encryption, restricted use of peripherals access, administrator restrictions and monitoring software.

"Advice from IT providers is that staff use weaker passwords if they have to change them too regularly."

An ICAEW firm

"We no longer require staff to change passwords; we now require multi-factor authentication and high complexity."

An ICAEW firm

Data security

98% of firms retain backups of data held, either locally, or off site or on the cloud. 87% have a data retention policy although this doesn't always comply with General Data Protection Regulations (GDPR).

Firms should hold personal data only for as long as necessary.

"Backups are stored in multiple data centres for redundancy and disaster recovery purposes."

An ICAEW firm

Incident management

73% of firms had specific cyber security insurance cover, with the majority of cover at levels of between £100,001 - £1,000,000 (49%) and £1,000,001 - £5,000,000 (32%). A small number of firms had cover of more than £5,000,000 (16%).

Levels of cover were generally set in consultation with the firm's insurer/ broker and internal discussion.

73% were aware that the Information Commissioner's Office (ICO) has agreed with the National Cyber Security Centre (NCSC) that it will look favourably on victims of nationally significant cyber incidents who report to and engage with the NCSC and that this might factor into its calculation of regulatory fines.

79% were aware of recent cyber-attacks on other organisations, including their own clients.

16% had suffered cyber-attacks, although these didn't in all cases result in data breaches. Of these, 84% reported the incident to government bodies such as the NCSC, ICO, HMRC and ICAEW.

2025 area of focus: cyber security continued

Incidents included individuals trying to intercept payment instructions, compromised shared mailbox access, access to email accounts and systems via phishing attacks (clicking on links in emails) and ransomware attacks.

"Payment fraud training has to be completed by all staff."

An ICAEW firm

74% reported the breach to affected parties such as clients or suppliers.

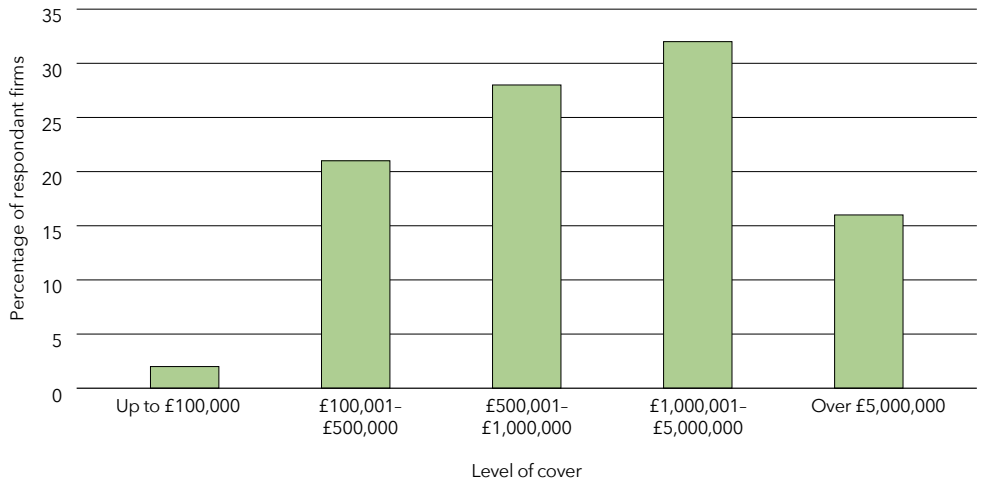
Following a cyber-attack leading to a data breach, 68% of firms involved third-party advisers or consultants and 58% involved their insurers.

Measures to prevent payment fraud include staff training, procedures to call suppliers to verify payment details and dual authorisation for payments.

"The rise of AI-driven cyber-attacks has made these threats more sophisticated and difficult to detect."

An ICAEW firm

Level of cyber insurance cover



Supply chain security

Not all firms share data with third-party suppliers. Those that do share or grant access to data to payroll providers, third-party software providers, website builders, IT support and data stores including cloud storage providers. 71% had protections over data shared with their supply chain.

71% of firms consider they know the security arrangements of their suppliers and routinely engage to ensure they are continuing to manage risks effectively. Assurance is gained through reliance on reputation of the supplier, but also in some instances through the firm's own due diligence, including enquiry and/or inspection of security certification. Only 32% had exercised their right to audit and/or require upward reporting from suppliers to provide security assurance.

"As part of onboarding a new supplier, there is a questionnaire to be completed by the supplier."

An ICAEW firm

45% had built assurance measures into their minimum security requirements, and 36% set minimum security requirements for suppliers although only 25% had these set out in their contracts.

"The firm's risk assessment is used to manage all third-party suppliers. This requires the suppliers to complete a six-monthly security questionnaire and then we monitor responses against our baseline to ensure no risks are identified."

An ICAEW firm

2025 area of focus: cyber security continued

Key reflections from ICAEW's Tech Policy Department

It is positive to see that the large majority of firms are aware of cyber security certifications such as Cyber Essentials. Maintaining up-to-date certificates like these are helpful in demonstrating to clients and other stakeholders that basic cyber controls have been implemented. However, they are often only a starting point and must be underpinned by strong cyber governance. Recent cyber incidents have demonstrated the importance of measures such as evidence-based oversight of supply chain risk, integration of cyber risk management into wider business risk management activities and testing of incident response plans.

Firms should ensure that they have the right governance in place to direct, resource and oversee their cyber security activities.

Cyber governance is becoming an increasingly important topic. Businesses are being encouraged to adopt the Cyber Governance Code of Practice – GOV.UK

Esther Mallowah
ICAEW Head of Tech Policy
(AI and Technology)

"Firms should ensure that they have the right governance in place to direct, resource and oversee their cyber security activities."

We recommend that firms implement procedures to mitigate the risk of cyber security incidents, for example:

- introduce governance measures eg, ensure cyber risk is recognised as a business risk (with ownership accordingly assigned to a senior business leader) and include cyber security in risk registers;
- align cyber security strategy to the organisation's business strategy;
- develop a suitable incident response plan and test it at least annually;
- conduct supplier risk assessments, set minimum security standards for suppliers and perform routine checks that they are continuing to manage risks effectively, put in protocols for new supplier set-up and change of supplier payment details;
- embed Cyber Essentials across supply chain;
- sign up to NCSC Early Warning;
- set controls over data exchange (eg, use of USB sticks, emails with sensitive data);
- conduct staff training and awareness; and
- monitor how breaches are identified and reported internally and to the ICO.

Resources

ICAEW guidance on cyber security
Cyber Essentials Accreditation scheme
Cyber Essentials Plus
Cyber Governance Code of Practice - GOV.UK

It's best practice to regularly review the nature and extent of your cyber insurance cover. If you do not already have appropriate cover in place, you should address this as soon as possible.

2026 areas of focus

We have chosen two areas of focus in 2026.

- Professional Conduct in Relation to Taxation (PCRT)
- Working with vulnerable clients

Professional Conduct in Relation to Taxation (PCRT)

PCRT is produced by seven professional bodies, including ICAEW, for their members working in tax. It sets out the high ethical standards which form the core of the tripartite relationship between tax adviser, client and HMRC. The latest PCRT responds to the government's challenge to the professional bodies to take a greater lead in setting and enforcing clear professional standards around the facilitation and promotion of tax avoidance. PCRT has been endorsed by HMRC as an acceptable basis for dealings between members and HMRC.

PCRT applies to all members providing advice on UK tax matters including employees of those members. The principles also apply to members' own tax affairs.

PCRT consists of the Fundamental Principles and Standards for Tax Planning for the provision of tax services and standards for tax planning that all members must follow. The current version took effect from 1 January 2026. The PCRT bodies also established a working group to draft topical guidance covering the application of PCRT to the requirements of Making Tax Digital (MTD) for Income Tax, in readiness for the mandating of MTD.

Members must be familiar with, and comply with, PCRT and a failure to do so may result in disciplinary action.

We have selected PCRT as an area of focus for 2026 given the recent update to the guidance and increased regulatory focus in this area.

> Information about PCRT

Working with vulnerable clients

ICAEW's Code of Ethics does not explicitly address working with vulnerable clients but the fundamental principles must still be applied. Firms should be alert to the indicators of vulnerability to aid in identifying actually and potentially vulnerable clients.

We have selected this as an area of focus this year, in view of the increase in the number of consumers displaying a characteristic of vulnerability and many of these individuals may have multiple characteristics of vulnerability. It is therefore likely that firms will have an increasing number of clients that are experiencing issues and require particular consideration.

> Information about working with vulnerable clients

> Guidance for firms on the fair treatment of vulnerable customers | FCA

We look forward to summarising our findings from these important areas in our 2027 Practice Assurance monitoring report.

Feedback from firms

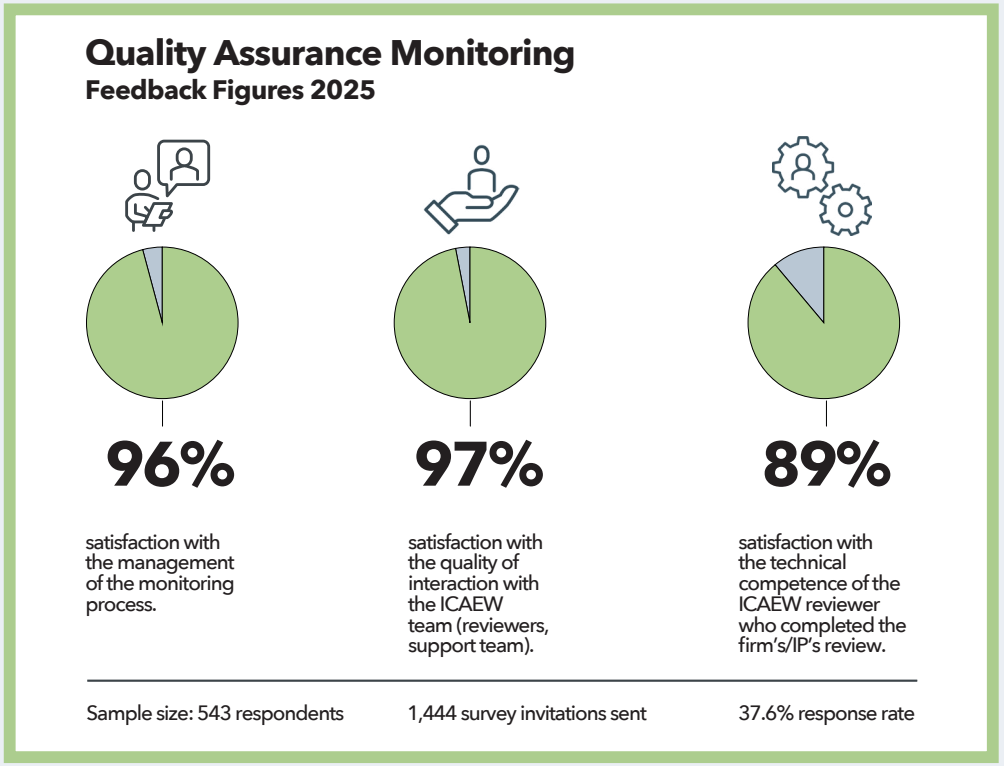
After each quality assurance monitoring review, firms are asked to complete an anonymous survey, providing feedback on the review process, the quality of interaction and the support provided.

These survey responses are collated and analysed by an independent research agency, and we receive a quarterly and annual overview report which we use to support the continuous improvement of our monitoring processes and procedures.

In 2025, 96% of firms were satisfied with how we managed the process, and 97% were satisfied with the interaction with our reviewers and the wider quality assurance team.

"The reviewer was exceptional. He blended confidence and calmness, while conducting a firm but fair review."

An ICAEW firm



"The reviewer quickly understood the nature of my firm and conducted the review accordingly, taking account of what was and was not relevant in my case. This made the review straightforward and painless with some good pointers to best practice."

An ICAEW firm

Help and support from ICAEW

Practice Assurance monitoring results 2026 webinar

(5 June 2026)

→ Technical Advisory Services helpsheets

→ CPD learning and resources

→ Practice Assurance resources

→ ICAEW library service

→ Practice Assurance Regulations and standards

→ Anti-money laundering resources

→ Core Accounting and Tax Service with Bloomsbury

→ Practice Assurance top tips and guidance

Helplines and support

Technical Advisory Services – for help with your technical questions
+44 (0)1908 248 250

Regulatory Support – for help with maintaining your firm record
+44 (0)1908 546 302

Appendix

APPENDIX 1: OVERSIGHT OF ICAEW'S REGULATION AND CONDUCT ROLES

ICAEW regulation and conduct oversight structure

All regulatory and disciplinary decisions are made by a lay majority or lay parity.

ICAEW's regulation and conduct role

Our role is to help ICAEW members and firms to maintain high professional standards and hold them to those standards. We act in the public interest to strengthen trust in ICAEW members and firms by raising standards through a programme of continuous improvement.

ICAEW's regulation and conduct roles are separated from ICAEW's other activities through internal governance so as to ensure the independence of all regulatory and disciplinary decisions. These roles are carried out by the Professional Standards Department and overseen by the ICAEW Regulatory Board and oversight regulators including the Financial Reporting Council, the Insolvency Service, the Office for Professional Body Anti-Money Laundering Supervision and the Legal Services Board.

We:

- **authorise** only those firms and individuals with the appropriate expertise and experience to undertake accountancy services regulated by law such as statutory audit, local audit, insolvency, investment business advice and legal services such as probate;
- **support** professional standards in general accountancy practice through our Practice Assurance scheme;
- **provide** robust anti-money laundering supervision and monitoring;
- **monitor** registered firms and individuals to ensure they operate in accordance with laws, regulations and expected professional standards;
- **investigate** complaints and hold ICAEW Chartered Accountants and students, ICAEW-supervised firms and regulated and affiliated individuals to account where they fall short of the required standards;
- **respond** and comment on proposed changes to the law and regulation; and
- **provide** educational resources and materials to help ICAEW members and firms comply with laws and regulations and maintain high professional standards.

Chartered accountants are talented, ethical and committed professionals. ICAEW represents more than 211,600 members and students around the world. 81 of the top 100 global brands employ ICAEW Chartered Accountants.*

Founded in 1880, ICAEW has a long history of serving the public interest and we continue to work with governments, regulators and business leaders globally. And, as a world-leading improvement regulator, we supervise and monitor around 11,500 firms, holding them, and all ICAEW members and students, to the highest standards of professional competency and conduct.

We promote inclusivity, diversity and fairness and we give talented professionals the skills and values they need to build resilient businesses, economies and societies, while ensuring our planet's resources are managed sustainably.

ICAEW is working towards becoming net zero, demonstrating our commitment to tackle climate change and supporting the UN Sustainable Development Goal 13.

ICAEW is a founding member of Chartered Accountants Worldwide (CAW), a global family that connects over 1.8m chartered accountants and students in more than 190 countries. Together, we support, develop and promote the role of chartered accountants as trusted business leaders, difference makers and advisers.

We believe that chartered accountancy can be a force for positive change. By sharing our insight, expertise and understanding we can help to create sustainable economies and a better future for all.

www.charteredaccountantsworldwide.com
www.globalaccountingalliance.com

* includes parent companies. Source: ICAEW member data March 2026, Interbrand, Best Global Brands 2024

© ICAEW 2026 METCAH20864 05/26

ICAEW
Professional Standards Department
Metropolitan House
321 Avebury Boulevard
Milton Keynes
MK9 2FZ, UK

T +44 (0)1908 248 250

E contactus@icaew.com

icaew.com/practiceassurance

Chartered Accountants Worldwide Member

disability confident COMMITTED

GAA Global Accounting Alliance

Onvero TIDE Silver Standard 2024/2025

ICAEW is working towards becoming net zero