PROFESSIONAL STANDARDS DEPARTMENT

2026 Practice Assurance monitoring results

5 June 2026

Agenda

- Overview of Practice Assurance scheme
- Monitoring review outcomes
- Common findings from 2025 reviews
- Feedback on 2025 area of focus
- Areas of focus 2026
- Resources available to help you
- Q&A

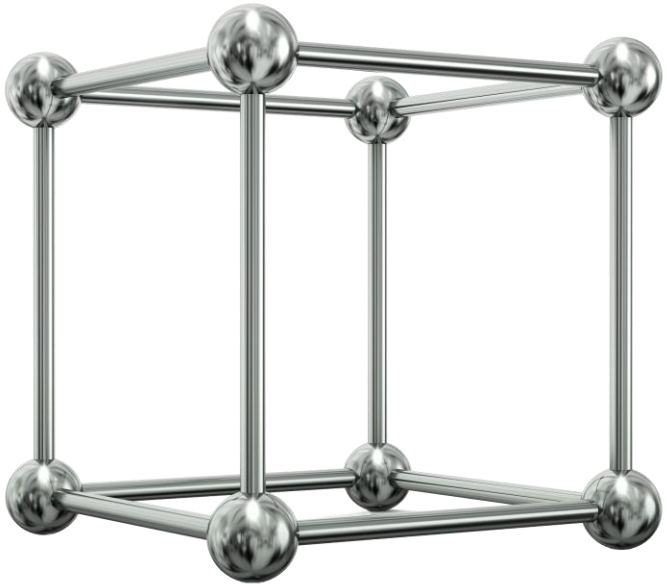
Overview of the Practice Assurance scheme

Principles-based quality assurance standards

Over 2,000 reviews in 2025

- New firm desktop reviews
- Telephone reviews
- On-site reviews
- Regional firms
- Large and mid-tier firms

Area of focus



Monitoring review outcomes

Monitoring review outcomes

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 – Analysis of 2025 findings

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

Common findings from 2025 reviews

Money Laundering Regulations

Key areas of non-compliance with the Money Laundering Regulations:

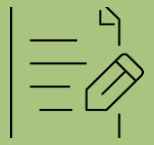
Customer due diligence (CDD)	Firm-wide risk assessment	Persons with Significant Control (PSC) reporting	AML training	AML compliance review

Access our web pages:

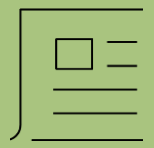
- ICAEW's AML Supervision report 2024/25
- AML resources | AML Supervision hub

Basis of fees and complaints, and engagement letters

We found that 273 firms had not informed their clients of the basis on which fees are charged and the 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.



See the ICAEW website: icaew.com/engagementletters

Clients' Money Regulations

Compliance with the Clients' Money Regulations remains one of the top areas.

- **109** firms that did not have a bank trust letter;
- **63** firms which had not carried out and documented an annual clients' money compliance review;
- **47** firms not using designated clients' money accounts when they held over £10,000 for more than 30 days;
- **41** firms were handling or holding clients' money which was not related to accountancy services.
- **33** firms had not followed correct procedures for taking fees from a clients' money balance; and
- **26** firms had not reconciled their clients' money accounts at least once every five weeks.

Referral fees and commissions

- We identified gaps in accounting for unregulated commission and/or referral fees at 158 firms.
- Things to consider:
  - Do you have enough information about the firm you are referring to?
  - Are you keeping a record of referrals / commissions received?
  - Have you obtained the necessary consent to retain commissions and notified your client of the amounts received?
- Access RQ's website: rq.app/icaew/rq

Professional indemnity insurance (PII)

Changes to the ICAEW PII Regulations that came into effect from 1 September 2024.

- The minimum limit of indemnity increased from £1.5m to £2m.
- For firms with a gross fee income which is below £800,000, the limit is two and a half times the firm's gross fee income, subject to a minimum of £250,000 (this is an increase from £100,000).
- Larger firms with gross fee income over £50m are not required to put in place 'qualifying insurance' but must have appropriate arrangements in place which will be monitored.
- For firms that will be 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.

Eligibility requirements

Use of description ‘Chartered Accountants’

Annual Return

Notification of changes

Access: icaew.com/firmrecord

ICAEW Code of Ethics

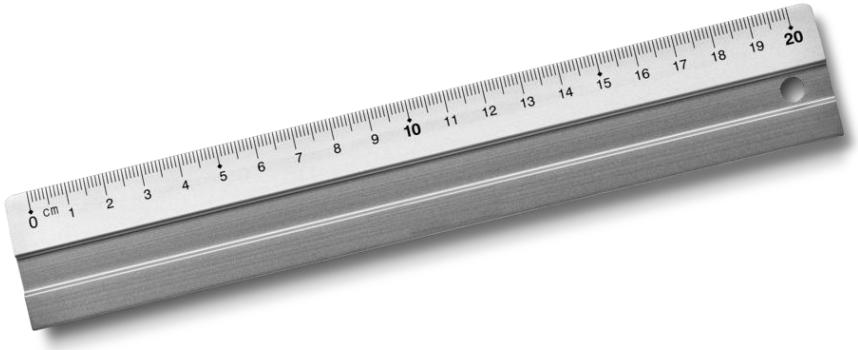
Threats to objectivity

Changes in the 2025 ICAEW Code of Ethics:

- Mindset
- Impact of technology
- Professional and personal conduct

Upcoming 2026 update:

- New sections on tax planning
- Relationship with Professional Conduct in Relation to Tax (PCRT)



Feedback on 2025 area of focus: cyber security

Awareness and expected impact

- **99%** of firms felt they had a good level of awareness.
- **99%** were aware of the Cyber Essentials certification scheme in the UK.
- **54%** had completed the Cyber Essentials basic self-assessment questionnaire.
- **29%** completed Cyber Essentials Plus.
- **38%** were aware of ICAEW's cyber security resource centre web pages.
- **15%** are certified under either the ISO27001 Information Security Standard or the Information Assurance for Small and Medium Enterprises (IASME) Cyber Assurance Standard.

Risk management

- 88% of firms (or their third-party IT providers) had used specific tools for security monitoring.

Risk assessments covering cyber security risks	Cyber vulnerability audit	Penetration testing	Investment in threat intelligence tools and resources

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

Engagement and training

Engagement

- **74%** of firms monitored assigned a principal / senior executive for overall responsibility for cyber security.
- **72%** of firms had a designated information security officer or equivalent.

Training

- **90%** of firms provided guidance to staff on cyber security matters.
- **82%** of firms trained staff on good cyber practices and awareness of most common attack methods.

System and access controls

Asset management

- **86%** of firms kept a list of critical assets.
- **81%** of firms had a contingency or business continuity plan in place.
- The majority for firms had policies and procedures for managing security risks.

Architecture and configuration

- **80%** of firms held critical systems on the cloud or a hybrid of cloud and onsite servers.
- **82%** of firms only permit access to systems through organisational devices.
- **79%** of firms use a VPN (Virtual Private Network).

Cyber security – policies for managing security risks

Risk factor requiring policies and procedures	Percentage of respondent firms
Homeworking	88%
Web applications	83%
Employee's use of own devices	81%
Use of wireless devices	79%

Data and identity controls

Vulnerability management

- **99%** of firms ensure that their systems are always up to date with the latest security patches.

Identity and access management

- Most firms had strong identity controls including password complexity requirements and widespread use of multi-factor authentication.

Data security

- Most firms regularly update systems and maintain data backups to reduce vulnerabilities and ensure resilience.

Cyber security cover

- **73%** of firms had specific cyber security insurance cover.

Incident management

16% of firms experienced cyber attacks in the last year, highlighting persistent security threats.

Of these, 84% reported the incident to relevant authorities, and 74% notified affected parties.

With 68% of firms involving third-party advisers or consultants and 58% involving their insurers.

Supply chain risk

Security

- **71%** of firms had protection over data shared with their supply chain.
- **71%** of firms consider they know the security arrangements of their suppliers.
- **36%** of firms set minimum security requirements for suppliers.

Reflections

Key takeaways and recommendations

- Large majority of firms have a good awareness of cyber security tools and resources.
- Awareness should be underpinned with strong governance, policies and procedures.
- Regular incident response testing and continuous staff training will enhance cyber preparedness and resilience.

Areas of focus 2026

Areas of focus 2026 – Professional Conduct in Relation to Taxation

PCRT

Recent updates to PCRT effective 1 January 2026.

Increased regulatory focus following government challenge.

Applies to all providing advice on UK tax matters.

ICAEW approach

Help firms consider how they become familiar and comply with PCRT.

Share best practice and signpost to relevant ICAEW and government resources.

Areas of focus 2026 –
Working with vulnerable clients

Vulnerable clients

Increase in number of vulnerable consumers.

Consider principles of ICAEW Code of Ethics.

Preparations to assist vulnerable clients.

ICAEW approach

Help firms consider how they can identify, prepare and deal with vulnerable clients.

Share best practice and signpost to relevant ICAEW and other resources

Resources available to help you

The Practice Assurance hub: icaew.com/practiceassurance

Practice Assurance resources: icaew.com/practiceassuranceresources

Find out more about our monitoring activities: icaew.com/regulation/practice-assurance/annual-return-and-monitoring

Practice Assurance fundamentals webinars: icaew.com/regulation/practice-assurance/fundamentals/what-you-need-to-know-webinar

Common pitfalls for firms: icaew.com/commonpitfalls

Cyber Security hub: icaew.com/cybersecurity

ICAEW

Stay informed

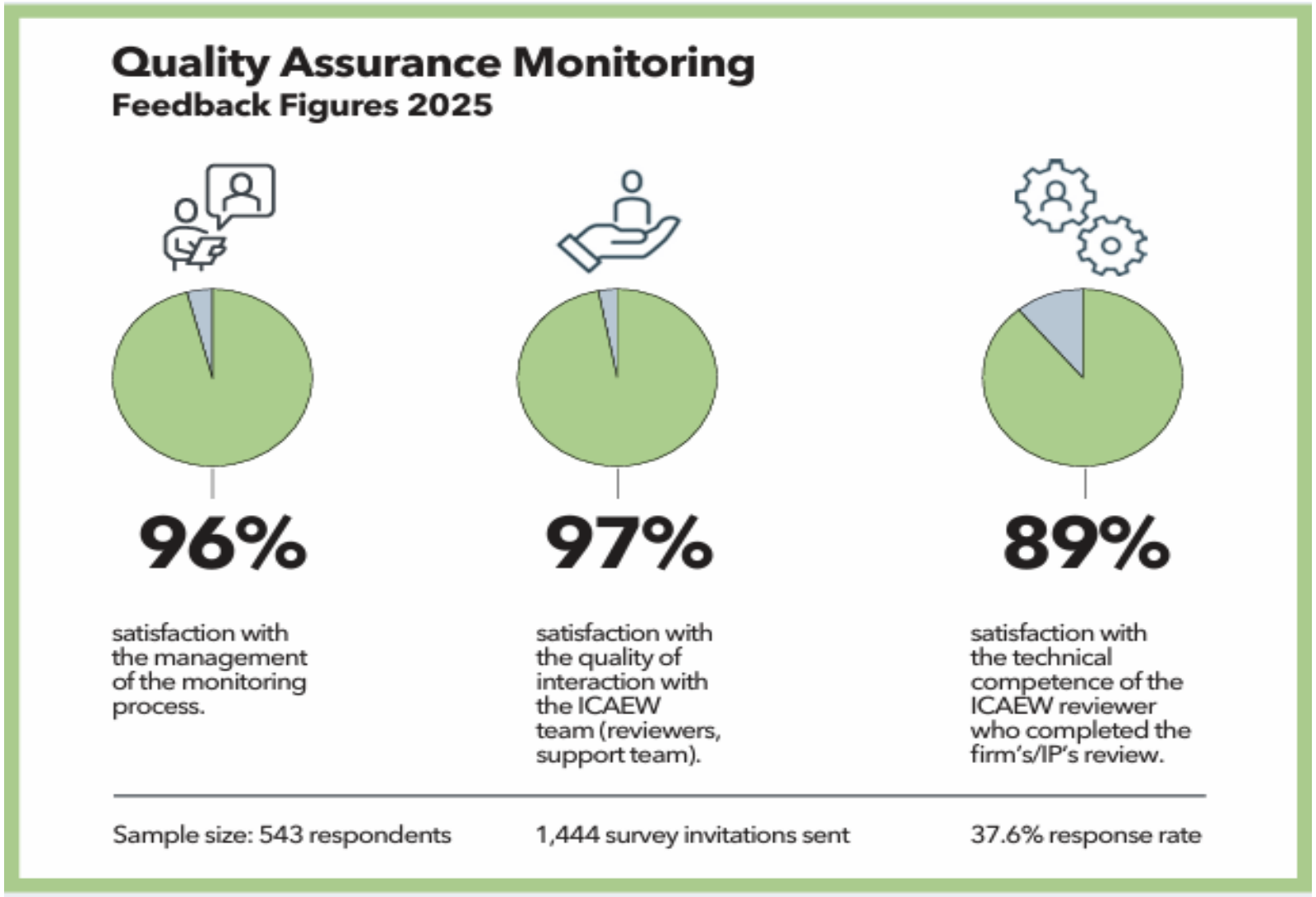
Sign up to the **ICAEW Regulation & Conduct News** e-newsletter: icaew.com/regulatorynews and follow us on our dedicated Regulation and Conduct LinkedIn channel

ICAEW Regulation and Conduct LinkedIn

Follow us for the very latest regulatory updates and guidance.

linkedin.com/company/icaew-regulation-and-conduct/

What firms are saying about their reviews



Q&A

icaew.com