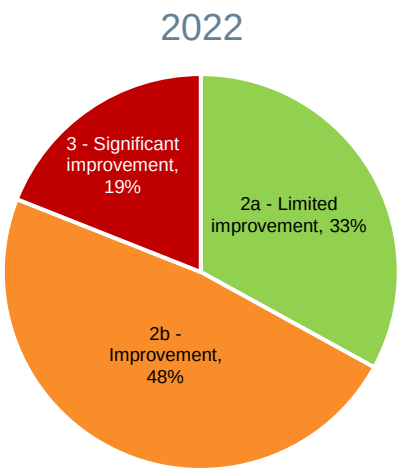
March 2023

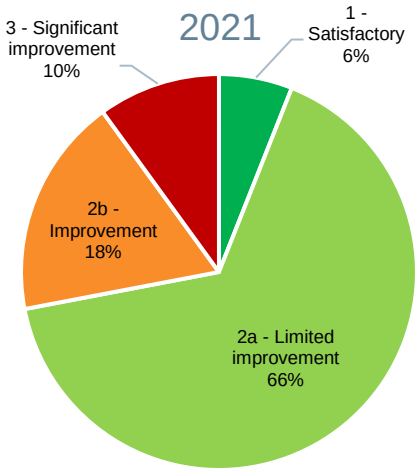
Audit Monitoring: 2022 & 2021 common findings

Audit Monitoring, common 2022 findings

2022 was an unusual year for ICAS Audit Monitoring, which saw a significant degree of change in the review team. As a result, there were fewer audit monitoring visits conducted with the 14 visits undertaken focusing on firms that had not been visited for six years. As the visit schedule was somewhat different to a 'typical' year, we expect that the visit findings might not be readily comparable to previous years. However, there are still key themes and common findings that all audit registered firms should take in to account and can learn from.

Every file reviewed in 2022 was considered to require some degree of improvement, with no files being considered a grade 1, or "satisfactory", standard. This was a concerning result, with 67% of the files requiring more than limited improvements. While a small number of 2022 visits were awaiting consideration by the ICAS Authorisation Committee at the time of writing, and as such have not yet been formally completed, initial findings are provided below for reference.





Most common International Standards on Auditing (ISAs) (UK) breaches

1. ISA (UK) 230 – Documentation (79% of visits)

Weaknesses in audit documentation remain extremely common in the files reviewed. Typical examples include working papers that do not clearly set out the nature and extent of audit testing conducted, or where the audit work had not been documented in sufficient detail to allow the audit monitoring reviewer to understand the results of the audit procedures performed, the conclusions reached, and the significant professional judgments made in reaching those conclusions. There were also instances where audit work, or supporting evidence, was held by the auditor but had not been added to the audit file.

2. ISA (UK) 500 – Audit evidence (71% of visits)

Obtaining sufficient appropriate audit evidence over all material transactions, balances, and disclosures is one of the fundamental requirements of the ISAs, and absolutely essential in conducting a quality audit. However, the monitoring team found weaknesses in audit evidence in the majority of visits conducted in the year. Common issues included:

- Material transaction streams, balances, and/or disclosures not being subject to dedicated substantive audit testing. Firms should be aware that, irrespective of the assessed risks of material misstatement, the ISAs require substantive audit procedures over each material class of transactions, account balance, and disclosures.

- Substantive testing being conducted in a way that does not properly address the audit risk identified. This included testing being conducted against the wrong assertion – such as sample testing designed to test the completeness of revenue being selected from the accounting records (and as a result testing the occurrence assertion).

- Areas of significant estimates and judgements not being adequately considered (eg the work of a management expert not being subject to sufficient consideration; or significant accounting estimates, such as those over construction contracts, not being considered under the full requirements of ISA (UK) 540).

3. ISA (UK) 315 – Risk assessment (57% of visits)

Reviewers regularly found areas where risk assessment procedures have not been adequate, with related breaches being raised in the majority of reviews. The most common driver for a breach of ISA (UK) 315 was insufficient audit work being conducted at the planning stage in order to understand, and document, the internal control environment relevant to the audit. This is often as a result of systems work not being documented over all relevant transactions streams (eg no system notes being held over payroll), or where the auditor has not determined whether the relevant controls identified have been implemented (eg a 'walkthrough' test has not been conducted, or has relied solely on inquiry of client).

4. ISA (UK) 240 – Fraud (50% of visits)

Half of the monitoring reviews conducted in 2022 found weaknesses in fraud considerations. These fell broadly under two categories:

1. Management's assessment of fraud risk had not been sufficiently considered and documented at the planning stage. Firms should ensure that, in addition to asking the client about known or suspected frauds, all audit files record:

    a) Management's assessment of the risk of material misstatement due to fraud;

    b) Management's process for identifying and responding to the risks of fraud;

    c) Management's communication, if any, to those charged with governance (TCWG) regarding its processes; and

    d) Management's communication, if any, to employees regarding its views on business practices and ethical behaviour.

2. Insufficient consideration of presumed significant risks relating to fraud in revenue recognition and from management override, due to one or both of these risks being omitted from audit planning, or the planned testing being insufficient in order to address the risk. In particular, reviewers regularly found that insufficient substantive testing had being conducted over journals and other adjustments in response to the significant audit risk from management override. Firms are reminded that every audit file should demonstrate:

    a) Inquiry of relevant individuals about inappropriate or unusual activity;

    b) Substantive testing of specific journals and other adjustments at the end of a reporting period;

    c) Consideration of the need to test journals and other adjustments throughout the period;

    d) A review accounting estimates for biases; and

    e) An evaluation of the rationale for significant transactions outside the normal course of business.

5. ISA (UK) 550 – Related parties (43% of visits)

A significant number of monitoring reviews identified non-compliance with the ISA requirements in relation to related parties. This typically reflected cases where audit planning had not sufficiently considered the completeness of potential related parties (eg where other interests of directors, or their close family members, had not been identified); where audit testing had not been conducted to ensure the completeness of related party disclosures; or where audit evidence had not been obtained in response to a management assertion that related party transactions were conducted on an 'arm's length' basis.

Common breaches of the Audit Regulations

1. Audit Regulation 3.10 - Compliance with the ISAs (UK)

See commentary above for common weaknesses in ISA (UK) compliance.

2. Audit Regulation 3.20 - Audit Compliance Review (50% of visits)

The Audit Compliance Review process is a key part of a firm's approach to audit quality. This internal monitoring becomes even more important under the new ISQM (UK) 1, so it is vital that firms invest time and effort to identify and improve on any deficiencies.

The findings during 2022 related to the old ISQC (UK) 1 and common issues identified in the year included:

- A formal Audit Compliance Review not being conducted, or the findings of a firm's review of compliance with the audit regulations not being consistent with that of the monitoring team (eg where the monitoring team had identified an issue with the firm's eligibility that was not identified in the firm's own compliance review process).

- A process of Cold File Reviews not being conducted in order to inform the firm's Audit Compliance Review, or weaknesses being identified in the firm's process. The most common issue in this regard was firms not conducting a Cold File Review process at all, which reflects a clear breach of the requirement. The monitoring team also noted instances where the findings of an internal Cold File Review process were not consistent with the findings of the monitoring team; and where firms had not sufficiently remediated issues identified by Cold File Reviews on subsequent audit files.

3. Audit Regulation 3.03 – Acceptance and reappointment (43% of visits)

Reviewers found breaches related to acceptance procedures in almost half of the reviews undertaken in 2022, with the majority of these relating to firms' consideration of ethical compliance at the outset of an audit. The FRC's Revised Ethical Standard 2019 sets out specific requirements relevant to ethical considerations that may arise in audit engagements, and compliance with the requirements of the Standard forms an integral part of every file review conducted by the monitoring team. Any breach of the Ethical Standard has the clear potential for the ICAS Authorisation Committee to take regulatory action. The most common weaknesses identified in 2022 were:

- Insufficient documentation being held at the outset of the audit demonstrating that Ethical Threats (such as the management, self-interest and self-review threats that commonly arise from the provision of non-audit service) had been identified, and that appropriate safeguards had been implemented in response; and

- Insufficient safeguarding of the threat from long association, where the additional safeguarding required by the FRC's Revised Ethical Standard 2019 had not been implemented. Firms are reminded that under the revised standard, a specific safeguard needs to be applied to the threat (in addition to communication of the matter to the client). Appropriate safeguards may include:

    i. Appointing another Responsible Individual ('RI') to lead the audit (something that may not be possible in some smaller audit firms);

ii. involving an additional partner, who is not and has not recently been a member of the engagement team, to review the work done by the partners and the other senior members of the engagement team and to advise as necessary (some smaller firms may not have another partner, independent of the audit team, with sufficient recent audit experience to conduct a review of this nature); or

iii. arranging an Engagement Quality Review ('EQR' as it's known under ISQM (UK)1 – this was previously known as EQCR under the previous ISQC (UK) 1) of the engagement in question (which may require an external reviewer to be engaged if a firm only has one RI).

4. Audit Regulation 3.08 – Statutory requirements (43% of visits)

These breaches reflect areas where disclosures made in the financial statements; or other areas of reporting, were found to be significantly deficient and/or where an accounting policy was found to be non-compliant which had not been identified through the audit process.

5. Audit Regulation 2.03 - Audit eligibility (14% of visits)

While less common, there have been a number of cases where firms have been found to have breached the eligibility requirements of the Audit Regulations as a result of principals not being appropriately notified to ICAS and/or affiliate applications not being submitted for principals that are not members of ICAS, ICAEW, ICAI, or ACCA.

Breaching the eligibility requirements is a significant matter, which will be reported to the ICAS Authorisation Committee, with the clear potential for regulatory action, such as a Regulatory Penalty, being proposed depending on the circumstances surrounding the breach. Firms are reminded of the importance that:

- ICAS is notified of all changes in principals on a timely basis (within 10 business days);
- Any principals of an audit firm who are not members of ICAS, ICAEW, ICAI, or ACCA will likely require an Audit Affiliate application to be submitted;
- Principals with the audit qualification must hold sufficient rights to direct the firm's overall policy or alter its constitution, ie at least a majority control (NB. If the firm is an LLP or an Unincorporated Partnership and has no formal partnership agreement, all members/partners will be considered to have equal voting rights).

CA House, 21 Haymarket Yards, Edinburgh, UK, EH12 5BH
+44 (0) 131 347 0100
connect@icas.com
icas.com

@ICASaccounting
ICAS – The Professional Body of CAS
ICAS_accounting
ICAS_accounting