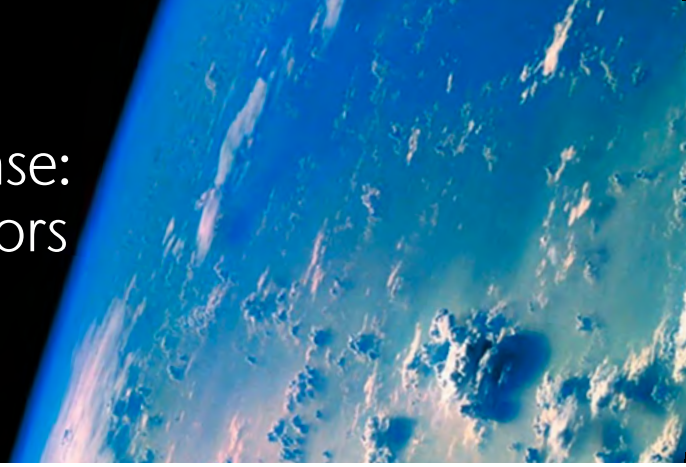
Risk assessment and the response: continuing challenges for auditors and issues for standard-setters



DOES EVERYONE AGREE ON WHAT 'RISK ASSESSMENT' MEANS?

Risk assessment has been critical to the conduct of all audits for a long time. 'Risk-based auditing' is a term often bandied about and a sure way to cast aspersions on an auditing standard or methodology is to assert that it is, 'not risk based'. Every time an auditing standard is revised, one of the purported benefits is that the new standard is risk based, implying that the extant standard is not. But the idea of a 'risk-based' approach to auditing has been around for at least 20 years, and it is not a difficult concept: it refers to the focus of the audit process on those areas that are most at risk of material misstatement.[1] Nevertheless, both auditors and regulators report problems in determining what constitutes a 'significant' risk, a 'material' risk and a 'high-risk area'.

The last major revision to the risk ISAs was finalised in 2003.[2] Those revisions precipitated significant adjustments to many firms' methodologies. Firms of all sizes initially struggled to apply the new requirements, and there was general agreement that while there was nothing inherently difficult about the new ISAs, they were unwieldy, not an easy read, and they were particularly hard to apply to smaller, less complex audits.

Despite the 'clarification' process in 2010, some believe that the risk ISAs are still unnecessarily lengthy, still hard to apply to smaller less complex audits and that they may be conceptually flawed, as well as out of date. They must accommodate very large audits in all their complexity, as well as the smallest of audits. While the changes made as a result of clarification in 2010 helped, and firms are now used to the language of the risk ISAs, problems applying them persist, and some problems pre-date all of these changes. For firms auditing smaller, less complex entities, one problem is the work required on internal controls as part of understanding the business, even when a wholly substantive approach is taken. We consider this in *Understanding the design and implementation of controls in smaller audits: why and how.*

WHICH ASPECTS OF RISK ASSESSMENT ARE CONSIDERED MOST PROBLEMATIC?

Appropriate risk assessments should be efficient in terms of cost and effort. If auditors, using their judgement, assess risk appropriately and make clear links between risk assessments and the procedures they perform, the audit stands a chance of uncovering material misstatements by focusing on the right areas. Corrections can be made to the financial statements if necessary and the audit opinion will be appropriate.

Linkages and judgement

Regulators note that the links between risk assessment, response and audit opinion might often be stronger.[3] It is not that auditors routinely fail to identify risks altogether, but rather that despite the fact that the risks are there for all to see on the file, their significance may not be understood, or they are not followed up.

Those responsible for audit quality within firms are concerned with risk assessment for several reasons. Firstly, it is fundamental to all audits. Secondly, there are many high-level qualitative terms (such as 'significant') used in ISAs to describe categories of risk and how they are to be dealt with, but it is down to audit firm methodologies to determine how these terms

1 This is not the same as risk management for audit practices which is about how firms manage their own exposure to risk.

2 The IAASB's clarity project made very limited substantive changes.

3 ICAEW's Quality Assurance Department (QAD) reports that weak risk assessment processes can potentially result in significant gaps in audit work, and in inefficiencies through over-auditing in insignificant areas. The QAD also notes that if firms reduce substantive testing based on the assessment of risk as 'low', the assessment must be properly supported with an adequate understanding of the client's business and control environment. The QAD finds that significant risks are not always identified as such and that auditor consideration of fraud risks sometimes appear to be little more than a compliance exercise.

are to be applied. Thirdly, there are natural variations within firms in terms of how audit teams interpret the requirements of ISAs and methodologies when identifying risks and determining the response required. Finally, even where the risk and response are clearly identified at the planning stage, there is sometimes an unwillingness to face up to difficult issues, which may result in auditors auditing 'around' them, because they are too complex, difficult or time consuming to address head on.

Furthermore, at each level, judgement is required. This extensive need for the exercise of judgement and to document it, challenges both audit regulators and those with responsibility for quality control within audit firms. Firms rightly defend the need for professional judgement, while emphasising the importance of consistency in the risk assessment, and the need to link risk to responses. But regulators seem to struggle with the fact that given the same set of criteria, different outcomes are often possible. Provided the different outcomes are within reasonable parameters, this should be acceptable but demarcating the parameters is a judgement in its own right requiring documentation in audit methodologies and on individual audits. Audit regulators, given their mandate, are likely to lean towards narrower parameters than auditors. The already fraught issue of determining acceptable parameters for quantitative measures, such as determining an acceptable range for accounting estimates, seems likely to become even more difficult as fair valuations with extended ranges of acceptable parameters, become more widespread.

What is a 'significant' risk?

Some difficulties in applying ISA requirements lie in the language used within the ISAs. For example, ISA 330 refers to assessments of risk as 'significant', and also uses terms such as 'high' and 'higher'. It is not clear whether a risk at an account or assertion level can be 'significant' without also being 'high', or vice versa, and variations in approach (at best) seem likely.

The IAASB noted in its post-implementation review of the clarified ISAs[4] (IAASB's review), which will form the starting point for its modernisation of the risk ISAs, that regulators are concerned about inconsistencies in auditor determination of what constitutes a significant risk. This lack of consistency may reflect misunderstandings among auditors or poor quality application of the ISAs, but it is also possible that ISA 315 is still not clear. ISA 315 defines a significant risk as one that, '...in the auditor's judgment, requires special audit consideration', and that in exercising that judgement, auditors take account of:

- whether the risk is of fraud;
- whether the risk relates to recent significant economic, accounting or other developments and therefore requires specific attention;
- the complexity of transactions;
- whether the risk involves significant transactions with related parties;
- unusual transactions including those outside the normal course of business; and
- subjectivity and the degree of measurement uncertainty.

It has been pointed out that while the factors to take into account may be helpful, the definition is both circular (a significant risk is one that needs to be treated as significant), and it focuses on how it is dealt with by auditors, rather than the substantive nature of the risk itself.

4 https://www.ifac.org/publications-resources/clarified-isas-findings-post-implementation-review.

HOW SHOULD AUDITORS BALANCE THE JUDGEMENTAL AND QUANTITATIVE ASPECTS OF RISK ASSESSMENT?

Auditors need to exercise judgement when assessing risk, but the use of judgement means that there will be variations in outcome. Audit regulators encourage standard-setters to develop guidance for auditors where they perceive that the exercise of judgement has led to inconsistencies, but they sometimes treat guidance as if it is mandatory by questioning approaches that deviate from that guidance, while at the same time complaining that guidance intended to help contain the level of variation sometimes becomes a substitute for the exercise of judgement itself. It can be hard to strike a balance here.

ISA 330 says that, '…assessed risks may affect both the types of audit procedures to be performed and their combination. For example, when an assessed risk is high, the auditor may confirm the completeness of the terms of a contract with the counterparty, in addition to inspecting the document.' Judgement is clearly required in applying this requirement and the effect of the assessment on the determination of the types and combination of procedures is highly subjective. But other ISAs suggest a more quantitative approach to risk assessment. For example, ISA 200 states that auditors use 'various approaches' to assessing risks, such as models that express '…the general relationship of the components of audit risk in mathematical terms to arrive at an acceptable level of detection risk'.

In practice, risk assessment always involves more than quantitative assessments. Where quantitative elements are included in firm methodologies, such as the percentages applied in assessing risk as 'high', 'medium' and 'low' for the purposes of sample size calculation, they are often intended as high-level boundaries designed to aid decision-making in borderline cases. They are not meant to be used rigidly or without thought. Quantitative elements in audit firm methodologies are certainly not written in stone (or in ISAs) and firms generally do not want them to be treated as if they were. Unfortunately, they sometimes are applied as if they were 'bright lines' and audit teams may, for a variety of reasons, be distracted by the mechanics of the firm's quantitative guidelines and focus on and document those, rather than the substance of the specific risk in hand.

For example, it is easy for auditors to get bogged down in the mechanical detail of a discounted cash flow exercise rather than taking the time to stand back and question the underlying assumptions and assess whether the cash flow makes sense in the context of the auditor's knowledge about the past performance of the business and in terms of the quantum and timing of returns expected. The mechanics may work, but the growth assumptions may be unreasonably optimistic, or inconsistent with past performance. Similarly, a firm's risk assessment may led a team to a small sample of items to be tested in a population of, say, expenses, but the team may mechanically test that sample without recognising that there are significant or unusual items in the population which merit attention.

If auditors do not both address and document the substantive, judgemental aspects of the specific risks in hand, as well as the quantitative elements of the firm's methodology, it is very hard to show how the audit procedures chosen address the risks. More seriously, if the nature of a risk is not properly understood or assessed because of an excessive focus on methodology, mechanics or the easily measurable, tests may not be properly designed, or even not designed at all, because teams may think that existing procedures cover the risk.

Reviewers considering the effectiveness of planning and team meetings sometimes find that a team has missed 'the elephant in the room', and has focused on the routine issues and overlooked the truly significant risks. These may be to do with fundamental threats arising from changes in the wider business and economic environment in which the entity

operates, from changes in technology or competition, or they may relate to the way the business is being managed, especially if it is being mismanaged. Auditors may want to avoid appearing to make business judgements because managing the business is not their affair, but business judgements sometimes affect the audit. Effective team planning meetings may involve all participants taking a moment to reflect on these issues, so that they are happy that they are not ignoring something that might well be obvious to a bystander.

ARE REGULATORS RIGHT TO BE CONCERNED ABOUT INCONSISTENCIES IN RISK ASSESSMENTS?

The use of a quantitative framework for risk assessment together with judgemental assessments such as 'high', 'medium' and 'low', are intended to facilitate consistency. The ISAs are also intended to promote consistency but it is equally clear that regulators think that there is a problem. The ISAs themselves may be part of the problem as may their application by auditors, but some concerns may also reflect regulatory distrust of the natural variations in outcome that the use of judgement inevitably entails. Teasing out these issues with a view to improving both real and perceived consistency is not straightforward and it is important that auditors, regulators and standard-setters do not simply make demands of each other to improve the situation.

In the UK, the Financial Reporting Council's (FRC) evaluation of the first year of extended audit reports[5] refers to consistency, as does IAASB's review, which identifies six 'key' themes, seven 'important' themes and a number of 'other' themes. Not surprisingly, these include risk assessment.

The 'key' themes in this area include concerns about inconsistency in the nature and number of significant risks identified in practice and the fact that the requirements to obtain an understanding of internal control can be difficult to apply. An 'important' theme is a concern that IT risks are not sufficiently addressed in the standard. The review notes that:

- inconsistencies in the identification of significant risks have an effect on work effort;
- the requirements to understand internal control and control activities relevant to the audit can be difficult to apply because auditors sometimes fail to link the controls they document to the risks they assess. More guidance on this linkage may be needed.

Some consider that the requirements in ISA 315 are excessive if, as in many smaller and less complex audits, a fully substantive approach to testing is adopted. Audit teams find themselves performing too much work on controls for which they perceive there is little benefit. It is therefore suggested that a better definition is needed of what 'relevant to the audit' means.

Regulators across a number of different jurisdictions, including the International Forum of Independent Regulators (IFIAR) and the FRC in the UK, have observed weaknesses in the way some firms deal with complex IT controls. It remains common for firms to audit around the computer rather than bringing in techniques that might be used to audit the 'box'. IAASB's review notes that this is not helped by the fact that ISA 315 is insufficiently reflective of the complexity of the IT and systems used by many larger entities. Some regulators believe that general IT controls may not be tested sufficiently when reliance is placed on IT-dependent controls because IT risks are not sufficiently emphasised in ISA 315. IAASB notes the critical importance of these systems to the audit, and concludes that the ISAs need modernising to reflect these complexities. This may not be good news for the audit of smaller, less complex entities unless the modernisation also recognises that

5 https://frc.org.uk/Extended-auditors-reports.pdf.

in some such audits, simple distinctions between the control environment and control procedures are all that is necessary, and that to apply the Committee of Sponsoring Organizations of the Treadway Commission (COSO) model to such audits may be inappropriate.

Other themes identified in IAASB's review cover the need for clarification or additional guidance on:

- 'risk assessment at the assertion level';
- 'documentation of risk assessment procedures': on the nature and extent of documentation for understanding the business and on internal controls, particularly for smaller audits;
- 'poor linkages between identified significant risks and the responses thereto', because responses sometimes appear to be generic;
- 'the work effort where risks are assessed as low': to address the excessive work performed in some cases;
- 'the meaning of material classes of transactions and account balances'; and
- 'internal controls generally': to deal with over-reliance on management sign-offs, inadequate testing of general IT controls, general concerns among regulators about how internal control testing is and should be conducted, a lack of appreciation of the benefits of an audit strategy involving controls testing, the limitations of high-level controls in relation to some account assertions, and the work to be performed when controls are tested on a rotational basis; and
- 'management override of controls'.

IAASB notes that complexity in the organisation of ISA 315 also needs to be addressed.

In its Work Plan for 2015/16,[6] IAASB states that 'information-gathering activities to inform future work' will be designed to seek further understanding of the findings above. There will be a staff-led initiative to gather information about the potential scope of a project. The plan suggests that co-ordination with firms and regulators will be necessary and that the way forward could include 'specific enhancements' to ISA 315, additional guidance or 'a more fundamental consideration of the implications', which may be shorthand for a complete re-write. There is to be an initial discussion at the IAASB's March 2016 meeting.

6 https://www.ifac.org/publications-resources/iaasb-work-plan-2015-2016.

 ISBN: 978-1-78363-381-4 TECPLM14239 11/15