Documenting and testing internal controls: issues that continue to challenge auditors

WHY ARE ISA REQUIREMENTS ON INTERNAL CONTROLS SO HARD TO APPLY?

Dealing with internal controls is, and always has been, an 'issue' in audits of all sizes for a number of reasons.

In smaller, less complex audits, one particularly long-standing issue is the extent of the required work on the design and implementation of controls where a fully substantive approach is taken. The major overhaul of the risk ISAs in 2003 only served to sharpen the focus on this problem. We deal with it in some detail in *Understanding the design and implementation of controls in smaller audits: why and how.* But there are many other issues that auditors struggle with when understanding and testing internal controls in audits of all sizes, including:

- deciding whether to test the operating effectiveness of controls;
- determining what constitutes a deviation and the tolerable deviation rate, and then dealing with deviations;
- revising the control risk assessment, and the effect of a revision on other audit procedures; and
- balancing the results of controls testing with substantive procedures.

Dealing with internal controls in larger, more complex audits is no more straightforward than dealing with them in smaller audits, but the issues are different. The IFIAR 2014 Survey of Inspection Findings[7] (the survey) reports the highest number of audit inspection deficiencies in three areas: internal control testing (24%), fair value measurements (20%) and revenue recognition (14%). The survey cites problem areas as including the audit of general IT controls, a lack of specialist IT expertise, and excessive reliance on 'tests of one'.[8] The survey does note improvements, but the area seems to be increasingly important, exacerbated by a lack of detailed guidance on the approach to application controls and how they relate to risk and the effectiveness of IT general controls. The survey notes that the use of IT specialists on complex audits is sometimes limited to testing IT general controls, and that testing IT application controls is often undertaken by audit teams who need more support.

The UK's FRC notes in its Audit Quality Inspections Annual Report 2014/15 (the report) that the work performed during the year as part of its Thematic Review of the Audit of Loans Loss Provisioning[9] (the review), showed deficiencies in the testing of the operational effectiveness of IT controls in a number of bank, building society and other audits. The report notes that significant improvement was required in the audit of IT controls. Common issues highlighted by the review included limited consideration of the impact of IT general control weaknesses and insufficient IT general control roll-forward procedures. The review also highlighted over-simplification of application control testing with excessive reliance on untested system-generated information, and on 'tests of one' in the absence of consideration of control attributes.

7 https://www.frc.org.uk/Our-Work/Publications/IFIAR/IFIAR-2014-Survey-of-Inspection-Findings.pdf.

8 'Tests of one' involve situations in which auditors believe that systems have not changed and a control is automated. The argument is that if the control works at all, it works every time, so testing it once should be enough. However, controls may have flaws that only give rise to an error in specific circumstances. For example, with a June period-end, if a bespoke accounting system automatically treats bookings as deferred income rather than income if they relate to months 7–12 in any year, bookings made for December of year 1 would be treated correctly as deferred, but those relating to the following January would be treated as current income.

9 https://frc.org.uk/News-and-Events/FRC-Press/Press/2014/December/FRC-publishes-review-of-audit-of-banks-loan-loss.aspx.

Some audit regulators are now recruiting IT specialists. Standard-setters, such as the IAASB, have recognised that auditing standards need to be modernised and firms are putting more resource into this area, as well as developing their data analytics capabilities.

At the other end of the spectrum, *Understanding the design and implementation of controls in smaller audits: why and how* discusses the need for auditors of smaller and less complex entities to document their understanding of the design and implementation of internal controls when they take a fully substantive approach to the audit. That article was authored by two individuals with extensive experience of UK smaller audits, Hugh Morgan of Baker Tilly and Michele Rose of BDO and ICAEW staff member Katharine Bagshaw. It involved wide consultation with auditors who serve on ICAEW's ISA Implementation Sub-group. Arriving at a consensus was exceptionally difficult because it seems that firms in different jurisdictions have very different approaches to the requirements of the risk ISAs in this area. Some take the view that there is little point in spending a great deal of time considering controls in smaller audits because they are not that relevant to the risk assessment process or the wider audit. But others take the view that ISAs require work on the design and implementation of controls relevant to the audit on all audits, not least in order to understand the business properly. Numerous examples of the types of controls typically found in smaller entities and their relevance to the audit are provided in the article.

In the light of these observations, it would not be unreasonable to infer that work on the design and implementation of controls in smaller, less complex audits may sometimes be inadequate. However, members of UK training consortia report that such work is sometimes excessive. All that is needed is sufficient work to enable auditors to understand the system, assess risk and design audit tests. It seems that too much work on important operational controls is sometimes performed, despite the fact that they are not relevant to financial reporting. Within a hotel group booking system, for example, technology has enabled hoteliers to fine tune changes to pricing on an hourly basis, based on algorithms applied to large amounts of data about competitor prices. Auditors do not generally need to understand how prices are set – fascinating though it may be – but they do need to understand the controls that ensure that the right price (ie, one extracted from the correct file subject to various parameter checks) is being charged, because this information will be used in substantive testing.

IAASB may wish to consider whether when modernising the risk ISAs, it should recognise that in smaller, less complex audits, simple distinctions between the control environment and control procedures are all that is necessary and that to apply the COSO model to such audits may be inappropriate.

WHY DOES UNDERSTANDING AND DOCUMENTING CONTROLS WITHIN SYSTEMS SEEM TO BE SUCH A PROBLEM?

The requirement to understand and document system processes and controls involves procedures such as talking to the client, internal control and internal control evaluation questionnaires, narrative notes and flowcharts. On larger, more complex audits some combination of these approaches is likely. For smaller, less complex audits with simpler controls, the extent of documentation and what is most appropriate in the circumstances are both important. Budgets are sometimes cited as a reason for spending less time and effort on documentation in such cases but efficiently prepared, comprehensive and up-to-date documentation probably costs less in the long run than out of date and incomplete documentation, because of the long-term effects on the efficiency of the audit approach, and in terms of regulatory consequences.

In very general terms, smaller, less complex audits tend to involve narrative systems notes. Documentation of systems generally tends to be underdone rather than overdone on all audits. Keeping it up to date – a housekeeping exercise – is often regarded as a chore rather than something with any intrinsic audit value, particularly where only minor changes are made. Provided the audit team does not change, this does not necessarily create problems on a day-to-day basis. However, incremental minor changes stack up and when the team does change, there is rarely any budget for a catching-up exercise. When a catch-up becomes unavoidable, it is not uncommon to uncover aspects of the system that are poorly understood with consequential inefficiencies, in terms of under or over-auditing.

Common failings in narrative systems notes include incomplete records of certain relevant control activities, such as how management accounts are prepared, how the budgeting system works, how journals are processed, how related parties and transactions are identified and approved, how supplier accounts are set up, the use of credit limits and the approval of expenses.

While narrative notes are usually sufficient to understand how a transaction is recorded in the general ledger, they can only be adequate for the purposes of identifying controls to prevent misstatements or manipulation if they are up-to-date, and if the preparer has given active consideration to the issue. Flowcharts may help, but well thought out and up-to-date narrative notes should suffice in most cases.

IN SMALLER, LESS COMPLEX AUDITS, DO AUDITORS REALLY NEED TO THINK ABOUT WHETHER TO TEST THE OPERATIONAL EFFECTIVENESS OF CONTROLS?

In smaller, less complex audits, there is often a theoretical decision to be made regarding whether to test the operating effectiveness of controls. It is very common in smaller audits for a fully substantive approach to be taken even though there are controls that could be tested, because it is quicker and easier. Sometimes though, this is simply a legacy of past practice and it may be worth reviewing the approach from time to time. Work to update and document the auditor's understanding of the design and implementation of controls has to be performed annually regardless, and that work can be leveraged if controls are tested.

In smaller, less complex audits, auditors may be reluctant to consider changing a fully substantive approach, despite the presence of functioning controls, because budgets may not accommodate such changes, for example, even though this may lead to long-term inefficiencies. Other reasons for sticking with the existing approach regardless of what has changed at the client include a fear of doing things differently, unfamiliarity with tests of controls or how to deal with deviations, or a more generalised unwillingness to invest in the future.

Situations in which a move from substantive to controls testing might be worth considering, and factors to take into account include:

- the implementation of extensive changes recommended in a management letter, combined with improved operating effectiveness in transaction cycles;
- significant other improvements to controls, such as the financial statement closing process;

- improvements in the technology available or the recruitment of more IT literate staff;
- the development of knowledge or skills within the audit firm through training or recruitment, bringing with it the confidence to try a change in approach;
- the formalisation and documentation of new controls by the client as a result of expansion, for example, which makes testing of those controls more feasible. However, the size of the entity is not the only factor to take into account and where larger audits remain less complex, a substantive approach may still be perfectly reasonable.

IS DEALING WITH DEVIATIONS FROM THE APPLICATION OF CONTROL PROCEDURES A REAL PROBLEM IN SMALLER, LESS COMPLEX AUDITS?

In performing controls testing, methodologies must help auditors determine what constitutes a deviation and the tolerable deviation rate. Statistical methods can be used when dealing with lower-level tests of controls. For higher-level controls, more judgement is required. It is the level of judgement required in dealing with deviations that gives rise to many of the problems in controls testing, particularly in some smaller, less complex audits.

For example, in not-for-profit organisations, a control over donations received by mail often involves the mail being opened by two persons. There is no real 'fully substantive' alternative to testing this type of control if this is the principal control that serves to ensure the completeness of income and the absence of fraud. If it is not effective, it can be difficult to obtain any other evidence to support the assertion. Testing the operational effectiveness of such controls is sometimes essential. Auditor observation of this procedure and a review of documentation evidencing the presence of two persons are two common tests of control. The opening of the mail by one person might constitute a deviation. How many times does this have to happen before the control ceases to be effective? Anything happening on a systematic basis is likely to be a cause for concern. The discovery that for half of the year it has happened once a week because one person has to visit a hospitalised relative might be an example. Other cases may not be so straightforward. If a review of a sample of documentation involves looking at one set of signatures of the two persons at random every other month, for example, what constitutes a tolerable level of deviation in this case? Less than 5% (when extrapolated) might be tolerable but even when that is unlikely to be exceeded, a considerable amount of additional work is probably required to show that errors are isolated, as ISA 330 does not permit auditors to assume that deviations are isolated, and effectively requires auditors to prove that they are not.

The tolerable level of deviation within automated systems is likely to be zero in many cases, but the tolerable level of deviation in the application of controls that require more human intervention is not, and requires more judgement.

REALISTICALLY, WHEN SHOULD AUDITORS REVISE THE CONTROL RISK ASSESSMENT? WHAT HAPPENS WHEN THEY DO?

When extrapolation of deviations from the application of a control procedure across the population exceeds the tolerable level, and/or further testing fails to provide evidence that supports an alternative conclusion that can be reconciled to the original evidence, auditors must conclude that the control is not operating effectively. This affects the control risk assessment, other tests of controls in the same area (there may be compensating controls), and subsequent substantive procedures. Substantively testing information from poorly controlled systems is an increasingly important issue in larger, more complex audits, as well as smaller audits.

Having to revise the control risk assessment upwards, particularly if it happens after the first year, causes problems because there is rarely, if ever, any contingency in the budget for the additional work required. The need for revisions would ordinarily become apparent during work on the design and implementation of controls during the first audit. If it does not, work on the design and implementation of controls may need to be improved.

WHAT DO AUDITORS NEED TO CONSIDER WHEN ADJUSTING SUBSTANTIVE PROCEDURES TO REFLECT THE RESULTS OF CONTROLS TESTING?

Some auditors struggle with the difference between tests to check that the auditors' recording of the design and implementation of controls is accurate, tests of the operational effectiveness of controls and related substantive procedures. This is partly because audit firm terminology sometimes uses terms such as 'walk-through tests', to describe any or all of these procedures, and partly because a single test can perform multiple functions. It is important to understand the nature of any particular test, however described, and especially its limitations. The tendency to overstate, rather than understate the various conclusions that can be drawn from a single test is almost universal.

Some firms put a lot of time and effort into work on the design, implementation and testing of controls in the first year, in the knowledge that this work should pay off in subsequent years, particularly if the firm decides to take advantage of the 'three-year' rule and rotate the testing of controls over this period. Applying the 'three-year' rule, however, is not always straightforward. ISAs do not permit it to be applied in areas of significant risk, and a 'proportion' of other controls must be tested each year, using a rotational approach.

The results of substantive analytical procedures are important in providing audit evidence to address the assessed risks, and in determining sample sizes. However, it is important to distinguish between substantive analytical procedures and analytical procedures performed for planning or review purposes, the performance of which are often erroneously taken to permit a reduction in sample sizes. Base-line sample sizes of 60, 90 or 120 items within some firm methodologies encourage the use of substantive analytical procedures to reduce those numbers. High base-line numbers such as these have arisen partly from regulatory pressure after the financial crisis and partly from a perceived over-reliance on judgement sampling.

The reduction in base-line sample sizes for substantive procedures when tests of controls show that controls are operating effectively typically range from 30% to 50%. Factors to take into account in deciding how much of a reduction can be made include the overall audit approach, the circumstances of the entity, the balance between substantive analytical procedures and other substantive procedures, and the nature of the associated risks.

All firms change their methodologies over time, including base-line sample sizes for both tests of controls and substantive procedures. The FRC is currently conducting a Thematic Review of sampling among larger firms. Changes in sample sizes are linked to changes to the balance of audit evidence sought from:

- tests of controls and substantive procedures;
- tests of high-level general controls and tests of more detailed control activities over transactions and balances; and
- substantive analytical procedures and detailed tests of transactions and balances.

Firms may also seek to make more use of substantive analytical procedures in an attempt to reduce the level of detailed testing of transactions and balances. Some firms have recently sought to improve efficiency by making better use of work on high-level general controls to reduce the level of testing on both lower-level controls, and the extent of substantive procedures.

Testing the operational effectiveness of high-level controls general such as controls over budgeting and management accounts, including the entity's own review processes, requires some thought. Evidence is needed to show that such processes can actually prevent, detect and correct specific material misstatements. This may not be straightforward, and the resulting reduction in substantive work undertaken may be fairly modest.

All of these trends are sometimes checked when it becomes clear that either the quality, extent and depth of evidence obtained from work on high-level general controls is insufficient to warrant extensive reductions in other types of testing, or when it becomes clear that, for whatever reasons, substantive analytical procedures are not being performed to a sufficiently high standard to warrant the hoped for reductions in detailed tests of transactions and balances. Firms seem currently more inclined to perform detailed tests of transactions and balances than to rely on substantive analytical procedures.

IS DATA ANALYTICS REALLY SOMETHING NEW AND IS IT REALLY GOING TO CHANGE THE WAY AUDITS ARE PERFORMED?

It is clear that the technology that permits auditors to test and manipulate large amounts of client data is being refined and is now being used on more audits. There will be increasing demand among firms and regulators for more IT-literate staff who are sufficiently confident to test controls over computers rather than working around them. Standard-setters are also under pressure to update auditing standards in line with these developments. The technology involved in data analytics is by any measure a step change from the computer-assisted audit techniques (CAATs) of yesteryear and the capabilities currently being developed by large firms do call into question a perceived assumption in the risk ISAs that not all of the transactions in a population will be tested.

All of the larger firms have made it clear that they are developing predictive analytic technologies. Some of these technologies were originally developed within the firms for forensic accounting purposes, including data mining software. Some involve the development of proprietary digital platforms. Some technologies are being developed in partnership with third parties. It seems that many are intended to apply to both advisory and audit services.[10]

10 The accountancy press has reported details of how the large firms are approaching data analytics. There are references to significant investments in automation, analytics and technological innovation, and to new technology being a core driver of innovation in audit. Some technologies were originally developed by forensics practices to help sift through unstructured data such as emails. By melding this with well-controlled 'structured data', firms are building up a more comprehensive picture of business operations to unearth anomalies. Some firms claim that social media have also created pools of data that could be relevant to an audit.

 ISBN: 978-1-78363-382-1 TECPLM14240 11/15

Understanding the design and implementation of controls in smaller audits: why and how

Risk assessment is key to an ISA-compliant audit, as highlighted in recent ICAEW Quality Assurance Department (QAD) monitoring reports. They recognise that firms often obtain sufficient evidence to address the risks, even though the risk assessment process itself may not meet all the requirements. The risk assessment process is important though, because without it, there is a danger that significant issues may be overlooked and the response to the risk assessment might not make sense. Standard work programmes help ensure that nothing is missed but they are much more likely to work if the risk assessment process that supports them is sound.

Consideration of internal control and of the risk of fraud are both areas in which auditors often need to improve their risk assessment processes. In particular, auditors need to remember that internal controls are still relevant where a fully substantive audit approach is adopted, and to be more sceptical about the risk of fraud at long-standing clients.

Understanding internal control and documenting that understanding is a challenge for all audits, irrespective of the client's size or complexity. In smaller, less complex entities controls are typically informal and undocumented, and potentially compromised by a lack of segregation of duties. However, the involvement of the owner-manager in the day-to-day running of the business can have a positive and a negative effect on the evaluation of risk.

The QAD has three tips for work on understanding controls as part of the risk assessment, and suggests that, even where auditors adopt a fully substantive approach, they should ask themselves whether they have:

- identified those controls that are relevant to the audit, such as those relating to the key transaction streams;
- checked whether those controls are designed appropriately to achieve their objectives; and
- obtained evidence that these controls have been implemented, by walkthrough tests, for example.

WHY IS WORK ON INTERNAL CONTROL NECESSARY WHEN AUDITORS TAKE A SUBSTANTIVE APPROACH?

Some auditors question the value of the work ISAs require on evaluating the design and implementation of controls. The purpose of this work is to help auditors properly understand the business and, very specifically, to deal with any risks arising from poor internal controls.

Performing the same substantive procedures, regardless of whether controls are designed, implemented and operated properly, poorly or not at all, ignores the following:

- ISAs require substantive procedures to be tailored to the assessed risks;
- a substantive approach often involves analytical procedures and if auditors ignore controls, they risk placing undue reliance on the information on which they perform the procedures, if it is produced by a poorly-controlled system;
- auditors may well miss something important in a key area if they do not understand that the controls over them are poor, and they may not be auditing in the most efficient manner possible if they do not understand that controls are good; and
- ISAs require auditors to obtain an understanding of the internal controls relevant to the audit by evaluating the design and implementation of those controls irrespective of the size and complexity of the client and regardless of the audit strategy.

WHICH CONTROLS DO AUDITORS NEED TO UNDERSTAND?

Auditors are only required to obtain an understanding of controls relevant to the audit. Controls relevant to the audit are typically controls over financial reporting. That is not to say that all controls over financial reporting are relevant to the audit. The only controls that auditors need concern themselves with are those that auditors believe may prevent, detect or correct a material misstatement. It is a matter of professional judgement whether a control individually, or in combination with others, is relevant to the audit. To be able to make this judgement, auditors need to understand the system within which the controls operate.

Internal controls in smaller and less complex entities are likely to be informal, but this does not mean that there will be no controls relevant to the audit or that if there are, they will never be good enough for auditors to test their operating effectiveness.

If auditors do not understand the system and assume that there are no controls relevant to the audit without further consideration, they write off the potential value of this work before they start.

Operational and financial controls are often tightly integrated and interdependent. In a theatre ticketing system, for example, controls over the issue of tickets are often linked with controls over the receipt of funds or the issue of invoices. This means that operational controls may sometimes be relevant to the audit and auditors need to think carefully about that and whether it is therefore necessary to assess their design and implementation. One way of determining this might be to ask whether the absence of the control might render the system inoperative, or vulnerable to the failure of a single control, or constitute a significant deficiency, for example.

CONTROL COMPONENTS

ISA 315 *Understanding the entity and its environment and assessing the risks of material misstatement* lists five internal control components:

1. the control environment;

2. risk assessment;

3. information system;

4. control activities; and

5. monitoring of controls.

The risk ISAs were introduced in 2003 using the five component classification of the US COSO framework. This framework has been widely used since 1992 and has stood the test of time. It was revised in June 2013, but the five basic components remain the same. ISA 315 does not require auditors to use it, provided that all of the components are covered, but many if not most firms and the providers of proprietary software systems find this a convenient framework to use.

CONTROL RISK ASSESSMENT

It is fair to assume that entities that are not dormant have some controls in place, however rudimentary. These controls need not be formal or formally documented; they just need to be appropriate for the entity concerned.

Auditors are required to perform some work to evaluate the design and implementation of controls in order to assess control risk. However, auditors cannot allow an expectation that controls are operating effectively to have any effect on the nature, timing and extent of substantive procedures unless the operational effectiveness of the controls is tested.