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.

Auditors may believe that controls are, or may be, operationally effective but choose to assume that they are not, and take a purely substantive approach. This may not be the most efficient approach but it is not prohibited. Nevertheless, ISA 315 requires auditors to substantiate the assessment of control risk in all cases and auditors cannot make any unsubstantiated assumptions about control risk simply because the entity is small. Even if auditors have decided to take a substantive approach, regardless of the quality of controls, and the control risk assessment has no effect of the nature or extent of procedures performed, ISA 315 still requires the control risk assessment to be performed.

KEY ISSUES FOR SMALLER ENTITIES

A lack of segregation of duties and the potential for management override are particularly important considerations for auditors of smaller, less complex entities, particularly those that are owner-managed. While the owner-manager's ability to closely supervise and oversee the business is potentially a strong control, in some situations this dominance can lead to the override of controls and the manipulation of financial data and business assets for personal objectives. Personal tax matters are usually important to owner-managers and provide the motive for bias in or manipulation of the financial statements. Auditors need to assess risks relating to the completeness of recorded assets and income in such cases.

Auditors need to understand the dynamics in place and the motivation of management to fully appreciate the nature and extent of potential risks of material misstatement. If auditors do not properly understand the design and implementation of its internal controls how can they properly understand the business, and if they do not properly understand the business, how can they design and perform the necessary further audit procedures?

OBTAINING AN UNDERSTANDING OF THE DESIGN AND IMPLEMENTATION OF INTERNAL CONTROL COMPONENTS: EXAMPLES

CONTROL COMPONENT	CONSIDERATIONS FOR SMALLER, LESS COMPLEX ENTITIES	EXAMPLES OF WORK ON CONTROL DESIGN AND IMPLEMENTATION
1. The control environment As part of obtaining an understanding of the control environment, auditors are required to evaluate whether: • management, with the oversight of those charged with governance, has **created and maintained a culture of honesty and ethical behaviour**; and • the strengths in the control environment elements collectively provide an appropriate foundation for the other components of internal control, and whether those other components are undermined by deficiencies in the control environment, such as the risk of management override.	The control environment is all about setting the tone at the top of an organisation, and influencing the control consciousness of its people. In many smaller entities, management and those charged with governance are likely to be the same – either the board of directors or the owner-manager, and may not include independent or outside members. However, with not-for-profit organisations the position is different because those charged with governance, such as trustees are often not involved in the day-to-day management of the business. The tone at the top can sometimes involve mixed messages and poor messages tend to have more impact than the good ones.	Auditors may obtain an understanding of the control environment in a smaller entity by **inquiry** of management or the owner-manager, by considering management's attitudes and motives based on prior experience and by **observing management's actions** during the audit. inquiry is an essential part of understanding an entity of any size but ISA 315 does not permit auditors to base their understanding of the design and implementation of controls on inquiries alone. Evidence from inspection, observation and walk-throughs is also required. Walk-through tests are particularly important in understanding implementation.

CONTROL COMPONENT	CONSIDERATIONS FOR SMALLER, LESS COMPLEX ENTITIES	EXAMPLES OF WORK ON CONTROL DESIGN AND IMPLEMENTATION
1. The control environment continued	Formalised policies such as a written code of conduct may be present in some smaller not-for-profit organisations but are less likely in other smaller entities. Even so, **a culture of ethical behaviour can be established through oral communication and leading by example.** If the tone at the top is good, **the owner-manager may exercise effective control over transactions which otherwise might be achieved through extensive segregation of duties** in a larger entity. However, if the tone at the top is poor, management override can easily occur and even the very best transactional controls over processes, such as purchases and revenue, can be overridden.	It is important to remember that understanding the design and implementation of controls is not the same as tests of the operational effectiveness of controls, although such tests are sometimes performed at the same time as work on design and implementation. It is often not possible to perform tests on the operational effectiveness of the control environment, but obtaining an understanding of the design and implementation of the control environment (and of all of the other control components) is critical to the control risk assessment. The tone at the top of a small, simple owner-managed business may be reflected in the extent to which the owner manager s**egregates personal assets and transactions from those of the business**. Owner-managers who make a clear distinction demonstrate a good tone at the top.
2. Risk assessment Auditors are required to obtain an understanding of the **entity's risk assessment process**, which is designed to • identify business risks relevant to financial reporting objectives; • estimate the significance of those risks; • assess the likelihood of the risks occurring; and • decide on actions to address those risks.	In a smaller, less complex entity, it is **unlikely that such a formal risk assessment process will be in place**. It is more likely that management will identify risks through their direct personal involvement in the business. If this is the case, or there is an ad hoc process, auditors may **discuss with management whether business risks relevant to financial reporting objectives have been identified and how they have been addressed.** Owner-managers are generally very aware of the risks facing their business. They simply see no need to write them down – but this does not mean that they have not thought about the risks to their business and made changes if they consider them necessary.	Auditors discuss business risks with management as part of the planning process and c**onclude on whether the risk assessment process in place is appropriate given the size and complexity of the entity**. The risk assessment process need not be formal or documented. It is unlikely that when auditors ask a smaller, less complex client about their risk assessment process that they will get a positive response. However, using more common terminology may result in a different answer. For example, instead of asking about business risks, auditors could consider asking the following: • what are the current threats to profits? • is the entity experiencing increasing costs?

CONTROL COMPONENT	CONSIDERATIONS FOR SMALLER, LESS COMPLEX ENTITIES	EXAMPLES OF WORK ON CONTROL DESIGN AND IMPLEMENTATION
2. Risk assessment continued		• how is the business performing against its competitors? • what impact has the current economic environment had on the business? Depending on the answers received, auditors will then need to ask how these issues have been addressed. Has the business cut costs, sought new suppliers, reduced their workforce, found new customers, or investigated new markets/territories, for example?
3. Information system Auditors are required to obtain an **understanding of the information system, including the related business processes, relevant to financial reporting**, including the following areas: • the c**lasses of transactions** in the entity's operations that are significant to the financial statements; • **the procedures, within both IT and manual systems**, by which transactions are initiated, recorded, processed, corrected, transferred to the general ledger and reported in the financial statements; • the related **accounting records**, supporting information and specific accounts in the financial statements; • **how the information system captures events and conditions**, other than transactions that are significant to the financial statements; and • **the financial reporting process** used in preparing the entity's financial statements, including controls over significant accounting estimates and disclosures.	Information systems and related business processes relevant to financial reporting in a smaller entity are likely to be much simpler than in larger entities, but no less important. Typically, the bookkeeping procedures and accounting records will be simple with no documented descriptions of accounting policies or procedures. Smaller entities generally use **off-the-shelf, accounting packages** with no modifications to produce their accounts. **Properly tailored good quality off-the-shelf packages operated by appropriately trained staff may well constitute a good quality control over information systems and accounting records.** For a smaller, less complex entity, **management and those charged with governance are likely to be the same body or person. Communication is likely to be informal and easily achieved** due to fewer levels of responsibility and management's greater direct involvement with the entity.	Understanding systems and processes may be easier in an audit of small entities. Auditors can gain a good level of their understanding of the information systems through **inquiry of management** and other relevant personnel and are less dependent on formal documentation such as client pre-prepared system notes. As before though, the understanding the design and implementation of systems should not be based on inquiry alone, and needs to be corroborated by reference to inspection of documentation, client staff observations on the operation of systems, and walk-throughs to ensure that systems have been implemented, and operates as prescribed, in accordance with the auditors' understanding. **Gaining an understanding of the accounting package, of the extent of staff competence and training, and of how well its security and other features are used also helps auditors assess risk.** Understanding obtained in prior audits and other audits of entities that use the same package can help auditors identify areas of risk that arise from the information system.

CONTROL COMPONENT	CONSIDERATIONS FOR SMALLER, LESS COMPLEX ENTITIES	EXAMPLES OF WORK ON CONTROL DESIGN AND IMPLEMENTATION
3. Information system continued • controls over journal entries, including non-standard journal entries used to record non-recurring and unusual transactions or adjustments are adequate. ISA 315 also requires auditors to obtain an understanding of how the entity **communicates financial reporting roles and responsibilities and significant matters relating to financial reporting**, including communications between management and those charged with governance and external communications, such as those with regulatory authorities.		An understanding of the communication processes will be most easily obtained though **discussion with management** supported by documentary evidence.
4. Control activities Auditors are required to obtain an understanding of **control activities relevant to the audit**, ie, those activities auditors judge it necessary to understand in order to assess the risks of material misstatement at the assertion level and to design further audit procedures responsive to assessed risks.	The concept of control activities is universal, irrespective of the size and complexity of an entity. Control activities are likely to be limited to the main transaction cycles such as revenue, purchases and payroll. Management's greater direct involvement in the day-to-day operations of smaller entities means that control activities are **likely to be less formal** than in a larger entity and rely more on **reviewing daily, weekly and monthly reports** on revenue, purchases and payroll, for example. **Automated controls within computer packages may provide some comfort on completeness and accuracy in the main transaction cycles** but they must be tested like any other control. Management's direct involvement in key decision-making is often an important feature of the management of any smaller entity.	Understanding control activities can be obtained **through discussion** with management and other staff, observation of their activities and inspection of documented controls, such as authorisations. Audit work might focus on **understanding how, for each of the main transaction cycles, a transaction is initiated, processed and recorded in the accounting system and reported in the financial statements**. Any lack of control activities, inappropriate design or failure to implement control activities will have an effect on the assessed level of control risk. It is more likely in this area than in any other, that tests of the operational effectiveness of controls will be performed. If such tests show that control activities are not operationally effective, the control risk assessment needs to be revisited.

CONTROL COMPONENT	CONSIDERATIONS FOR SMALLER, LESS COMPLEX ENTITIES	EXAMPLES OF WORK ON CONTROL DESIGN AND IMPLEMENTATION
4. Control activities continued		Where management makes key decisions and has the ability to intervene at any time to ensure an appropriate response to changing circumstances, auditors may decide that this control is sufficient to prevent or detect and correct material misstatements. There would be no need to consider more detailed control activities as part of the risk assessment process in such cases. For example: • if management has sole authority for granting credit to customers and approving significant purchases, it might constitute a strong control over important account balances. Auditors might consider that these two controls are sufficient and would not seek to identify further control activities in these areas; and • for a company holding a single leased asset with no indicators of impairment, management might use the lease contract as evidence of the assertions underlying the disclosure of the asset in the financial statements. There may be no specific controls relating to the asset other than management's knowledge and use of the lease contract. Auditor documentation of the use of the contract as the control over that asset may be sufficient for risk assessment purposes. It may not be necessary to investigate more detailed control activities in this area.

CONTROL COMPONENT	CONSIDERATIONS FOR SMALLER, LESS COMPLEX ENTITIES	EXAMPLES OF WORK ON CONTROL DESIGN AND IMPLEMENTATION
5. Monitoring of controls Auditors are required to obtain an understanding of the major activities the entity uses to **monitor internal control over financial reporting**, including monitoring of relevant control activities. They are also required to understand how the entity initiates **remedial actions** to correct deficiencies in its controls.	In a smaller entity, management's monitoring of controls may be through **management's own close involvement with the operations of the entity**. This may be through a **review of**: • **any management accounts** and significant variances; • **key performance indicators** set by management; and • **errors** in financial data leading to remedial action. It is important to recognise that in very small entities, where control is achieved through management's day-to-day involvement in the running of the business, it may not be possible for management to monitor controls because it would be effectively monitoring itself.	Auditors can obtain their understanding of management's monitoring of controls by**inquiry of management and inspection of items monitored** such as completed bank reconciliations. Evidence of changes made in prior years as a result of monitoring may also be relevant. The absence of effective monitoring controls is not necessarily fatal as other controls may be sufficient to reduce control risk to an acceptable level.

 ISBN: 978-1-78363-431-6 TECPLN1442611/15