

# How to achieve an appropriate control environment?

## Which is the right level of control for your company?

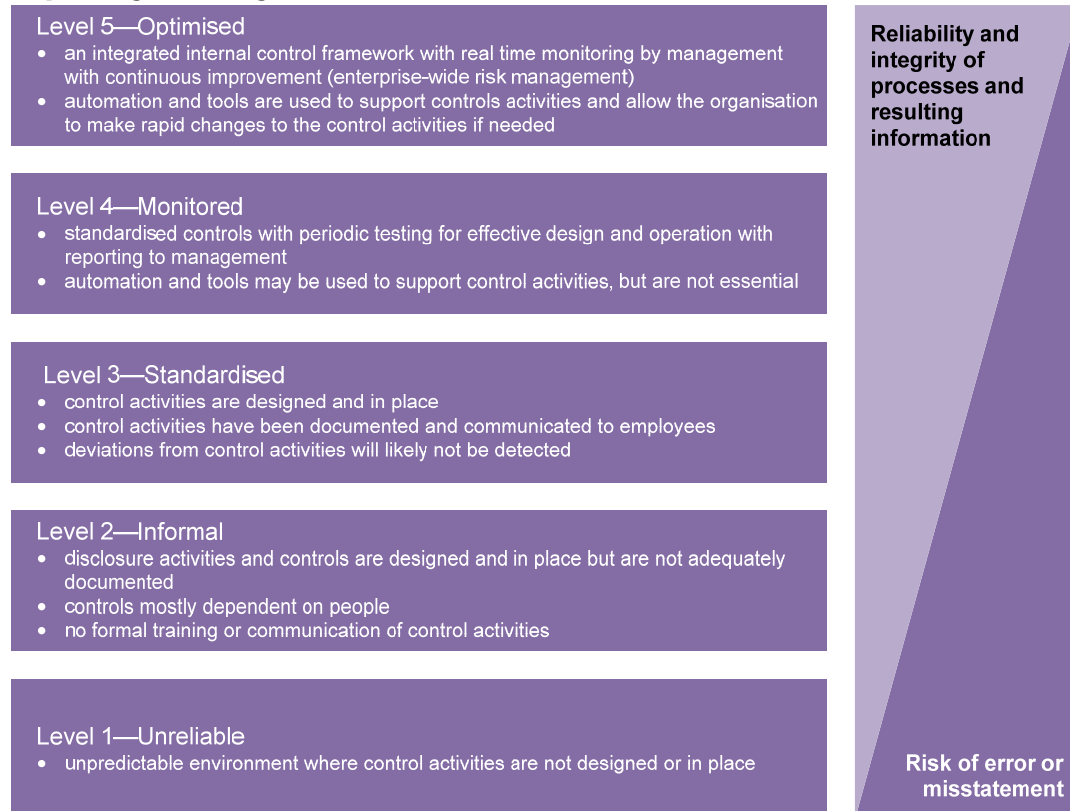
### Dispelling common myths.

#### What is a “reliable” control environment?

A reliable control environment is one where management places reliance on controls to mitigate business and financial statement risk. This reliance is based on periodic testing for effective design and operation of controls.

Controls evolve through a series of maturity levels, as organisations employ a disciplined approach to the design and periodic assessment of the operating effectiveness of related business processes. This can be illustrated as follows:

#### Capability maturity model



## **Capability maturity model—level 2**

Most large private companies have a level 2 control environment, i.e. they do have controls, but these are not documented or formally communicated. Management may gain some comfort from the presence of these controls, but there is no real assurance that the controls are effectively mitigating risk. In fact, given the lack of documentation of controls, there is no guarantee that management and the staff members operating the controls share the same understanding of how the procedures should operate.

A substantive external audit approach is the only alternative for a company at level 2.

## **Capability maturity model—level 3**

Achieving level 3 requires a company to standardise and document its controls and effectively communicate this to all ‘control operators’ i.e. the staff who execute the control procedures. This reduces the likelihood of inconsistent interpretations of how controls should operate, helps to ensure that the performance of controls survive personnel changes and provides a better platform on which management can base its assurance that risks are being mitigated. This assurance is limited by the fact that there is no formal periodic testing of prevent controls by management. However, it is very likely that management have implemented detect controls.

A controls-based audit approach is possible at level 3, where the detect controls are considered sufficient to provide assurance to management that business and financial statement risks are effectively being mitigated. However, in the absence of any formal testing of detect controls by management, there is a risk that the auditors will find control exceptions which may result in increased substantive audit procedures.

## **Capability maturity model—level 4**

Achieving level 4 requires management to implement a formal testing programme to support reliance on controls as effective risk mitigants. This testing must cover the design of the controls (to ensure that they are sufficiently robust to mitigate risk) and the operation of the controls (to ensure that they operate as documented consistently and without undetected exception).

At this point management must ensure that they take a sufficiently broad approach in the design of the control framework. Although the external auditor will be primarily concerned with controls over historical financial reporting and the risk of financial misstatement, management should be concerned at controls over all significant business processes, and all risks that could result in a material loss to the company and its shareholders.

A controls-based audit approach is not only possible but preferable at this level. If the controls are effectively designed and operating, and there is sufficient documentation and evidence to demonstrate this, then management (including any internal audit function) and external auditors can gain assurance from the same control framework. The value in being at level 4 is that it supports a co-ordinated enterprise-wide approach to mitigating risk that encompasses both external and internal audit functions and provides a much higher level of assurance to shareholders that their return on investment is being maximised. This is the required minimum standard for a Sarbanes Oxley (SOX) compliant company.

## **Key prerequisites**

A key pre-requisite of developing a control framework from level 2 to levels 3 and beyond is understanding which controls are required. A fatal mistake is to assume that the controls that already exist at a procedural level in the organisation will suffice, and to merely document and formalise these existing controls without challenging their appropriateness.

## **Prioritising processes and risks**

An efficient and effective control framework can only be created by firstly ensuring there is a clear understanding of the risks faced by the organisation. This is best done by prioritising the most important processes, and in turn prioritising the risks to the achievement of the objectives of those processes.

## **Matching controls to risks**

Once the risks facing the organisation have been agreed, understood, prioritised and documented, management has the information it needs to design controls (or choose existing controls) that are effective in mitigating those risks. At this point it is very common to discover that, not only are there risks that are not being effectively mitigated, but that there are existing 'controls' which are not mitigating any important risks and therefore consuming resources unnecessarily.

The control procedures designed and implemented at this point should be proportional to the risk and should ensure that risk is mitigated to a level acceptable to management and shareholders. In risk management terminology, the 'gross' or 'inherent' risk is mitigated to a 'net' or 'residual' risk level that is consistent with the organisation's 'risk appetite'.

## **Formalising and implementing the controls**

The most important aspect of this is communicating the controls clearly and unambiguously to all staff involved in operating the control framework. This requires explicit documentation of the controls and associated process and procedures. The level of detail should be sufficient for guidance and to avoid ambiguity, but should not be so excessive that it is difficult to keep documentation up to date and relevant.

## **Making sure the controls can be relied upon**

Even with a documented control framework, there is a significant risk that over time, operational practices will diverge from the 'official' documented procedures. This can be worse than having no documentation, as management may have a false sense of security from controls which they think are in place. The only effective way to ensure this does not happen and to detect deviations from the documented framework is to test the operation of the controls.

Testing of controls can confirm to management that it is appropriate to rely on those controls, but this is dependent on appropriate evidence of control operation being retained, and on this evidence indicating that there were no undetected control failures.

## **Dispelling common myths**

### **"Most companies already have a 'reliable' control environment"**

As detailed above, a 'reliable' control environment is one where management places reliance on controls to mitigate risk. This reliance is based on positive results from testing of key controls (which may be prevent controls). While most large private companies do have controls, these may not be documented or formally communicated, or no formal testing programme has been implemented to support the reliance on controls as effective risk mitigants.

### **"Only large companies have the resources to do this"**

Many large private companies are very professionally run, with controls designed and put in place. These companies are falling short of having a reliable control environment because they have not formalised the control framework through documentation and communication or through periodic testing for effective design and operation of controls. The key to a cost-effective transition to controls reliance is in prioritising the most important processes and risks, and formalising the controls that relate to these. Although it may be necessary to invest resources

in a project to design and implement an effective and efficient control framework, taking the opportunity to redesign controls for efficiency should make this initiative pay for itself very quickly.

**“It requires a huge quantity of documentation”**

A well designed control framework, where processes and risks are prioritised and controls are then matched to those risks, should be documented in sufficient detail to provide guidance and avoid ambiguity, but should not result in excessive documentation which is difficult to keep up to date and relevant. In short, any process which is worth doing is worth documenting in sufficient detail to ensure it continues to be done correctly.

**“It makes the business very detail-oriented, procedural and inflexible”**

This has not been borne out by the companies who have applied the resources to achieve a reliable control environment. A focus on efficiency as part of a project to transition to controls reliance will achieve a balance between allowing sufficient flexibility to operate a business, whilst limiting opportunities to violate controls.

**“It cuts audit fees / saves time on audits”**

While it provides for a better value audit, giving management and shareholders a higher level of assurance that can only be gained by having a reliable control framework, it will not lead to reduced audit fees or reduced audit time. The complexity of a controls-based audit (CBA) changes the mix of audit time and expertise, leading to more partner and manager resources used on CBAs. The real benefits to management and shareholders come not from changes in audit fees but from better management of risk in the organisation.

**“The Big 4 are using a CBA approach on most of their clients”**

All accounting firms which audit SEC registrants are required to use a CBA approach on those clients; however the control environment in most large private, non-SEC registrant companies, regardless of who audits them, is at level 2 or 3 of the capability maturity model and thus not likely to be reliable enough to facilitate a CBA approach.

**“Grant Thornton doesn't use a controls based audit approach”**

Grant Thornton has broad and in-depth experience of implementing a CBA approach in a wide range of industry sectors, including all Sarbanes-Oxley affected clients (SEC registrants) where we have acted as auditors or compliance and control advisors.

**Contact**

**Cian Blackwell**

Partner

T +353 (0)1 6805 710

E [cian.blackwell@grantthornton.ie](mailto:cian.blackwell@grantthornton.ie)

**Kathleen Ruane**

Director

T +353 (0)1 6805 670

E [kathleen.ruane@grantthornton.ie](mailto:kathleen.ruane@grantthornton.ie)

24-26 City Quay, Dublin 2

Offices also in Limerick and Kildare

This briefing is provided for general information purposes only and is not a comprehensive or complete statement of the issues to which it relates. It should not be used as a substitute for advice on individual cases. Before acting or refraining from acting in particular circumstances, specialist advice should be obtained. No liability can be accepted by Grant Thornton for any loss occasioned to any person acting or refraining from acting as a result of any material in this briefing. [www.grantthornton.ie](http://www.grantthornton.ie)