Management Systems

By Wiliam List CA Hon FBCS CITP, W^M. List & Co (W.List@ntlworld.com) *and Dr David Brewer, Gamma Secure Systems Ltd* (www.gammassl.co.uk)

This article was first published in eChartech from the Institute of Chartered Accountants in England and Wales, IT Faculty, December 2004.

Introduction

In previous articles we have discussed the effectiveness of internal control systems (Chartec July), proposed a methodology for documenting a risk treatment plan (Chartec August) and have considered how to measure the real effectiveness of an internal control system (Chartec October). In this article we show how the Audit Practices Board model of internal control can be realised in practice.

The APB Model

Following the publication of the Turnbull Report, many organisations requested advice on how its recommendations on internal control could be implemented. The Audit Practices Board responded with a document entitled "Briefing paper – Providing Assurance on the effectiveness of Internal Control". It proposes a model (see figure 1) that is both sound and practical:

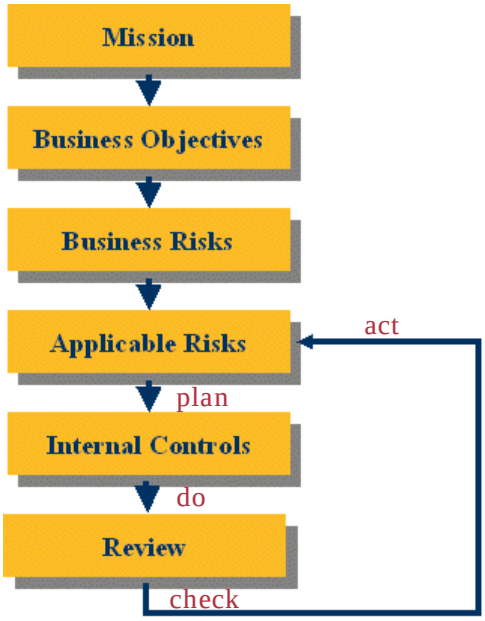

Figure 1: The APB model of internal control

- It is predicated on risk management. Controls cost money. If an organisation would loose money by not having the control, or alternatively would make more money by having the control, then the control is worthwhile. It is all a question of risk and risk appetite.

- It employs the Deming Cycle[1] – plan, do, check, act. There are many situations where we all do the "plan" and "do", for example in making our pension arrangements when first setting out in life – but do we ever do the "do" and "check" activities? It is these activities that police the internal control system and ensure that it is meeting its objectives.

[1] W. Edward Deming was a 1950s teacher who developed W.A. Shewhart's original three-stage model from the 1920s into the PDCA cycle, as a continuous quality improvement model. Although originally intended for industrial production processes this cycle applies equally well to 21st century business strategy in general and to our specific internal control management needs.

Management Systems

The Audit Practices Board model offers an approach to establish and police a sound system of internal control, but what are the controls that ensure that this is done? In ISO circles, the answer is a “management system”. In other words, a management system is that component of an internal control system that allows management to establish and police the internal control system as a whole.

The concept is embedded within COBIT and a variety of other standards, such as ISO 9001, ISO 14001 and BS 7799-2. Of all of these, BS 7799-2 is the most interesting. Albeit that it is a specification for an Information Security Management System (ISMS), but it is a very close fit to the Audit Practices Board model. Not only does it embrace the Deming Cycle, but it also embraces the concept of risk management. The other standards do not do this or do it so well.

BS 7799-2

Figure 2 presents the fundamental requirements of the standard set against the backdrop of the PDCA Deming Cycle. Being an information security standard it refers to security incidents, but its extension to being the specification for the management system of any internal control system in general is easily accomplished by interpreting an incident as being the occurrence of an impact. We spoke about impacts in the August Chartec.

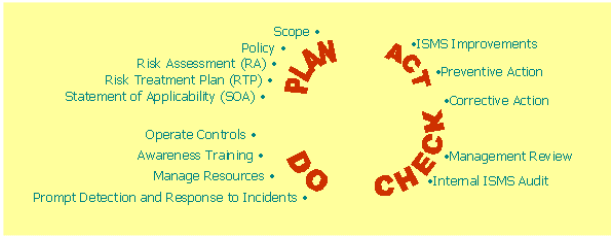

Figure 2: The management system requirements of BS 7799-2

Control Checklists

Built into BS 7799-2 is a control checklist (the Statement of Applicability) that addresses the issues concerning information security. It is not confined wholly within IT and addresses personnel, physical, environmental, legal and compliance issues as well. Most importantly, an organisation does not have to implement all of these controls. The standard recognises that some controls might be non-applicable and others, in addition to those covered in the standard, by be required. Other control checklists, e.g. for controls in specific business applications including the book keeping and accounts preparation can therefore be added at will.

Conclusion

In conclusion, a question to ask is “does your organisation have a recognisable management system within its system of internal control?” If not, BS 7799-2 could be a good place to start.