Effectiveness of Internal Control 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, July 2004.

Introduction

An Internal Control System (ICS) is fundamental to any business. In small businesses the 'boss' can run everything himself. Whilst a system would be helpful it is not a necessity. In larger organisations it is essential and in very large organisations middle rank managers are responsible for the system. Today there is pressure to ensure the ICS is effective as part of the Corporate Governance initiatives.

What does an ICS achieve?

The ICS is the system which enables management to implement the business mission and ensure that the implementation is correct and complies with the applicable laws and regulations. No system will ever be perfect therefore an essential ingredient of any ICS is to be able to detect failures and limit the consequent damage of such failures to the organisation. Excellent ICSs have achieved a balance of cost of deploying the controls such that the level of residual failures is manageable.

The effectiveness of the ICS involves measuring the time it takes to find failures and the time taken to rectify the damage. This measure is wholly under the control of the organisation whereas other metrics (e.g. computer malware caught by Intrusion detection software, the number and value of frauds by cashiers, the failure of debtors to pay their bills etc) whilst useful measure the external pressures on the ICS not its performance.

How is an ICS organised?

There are four steps in the construction and maintenance of an ICS. These are:

Plan - determine what procedures and controls are required to run the business, including those necessary to detect where procedures and controls perform inadequately or do not address current business requirements
Do – implement the planned procedures and controls
Check – monitor the performance of the procedures and controls.
Act – modify the system to take account of failures, changes in circumstances, etc.

This is known as the PDCA cycle and is the basis on which management systems in the ISO standards are based

How is a system created?

The greater the involvement of the senior managers in the development of the ICS the greater the probability is that resulting system will achieve the organisation's goals.

ICSs should be developed using risk analysis such as that recommended in the APB briefing paper 'Providing assurance on the effectiveness of internal control' published in July 2001. Often organisation start by using a baseline of common procedures (e.g. passwords to access computers, balancing ledgers, accounts presentation checklists, etc) to implement minimum controls over the procedures and augment the minimum controls as necessary once the risk analysis has been done.

The objective of all risk analysis methods is to identify the risks to meeting the business objectives and then identify what procedures and controls are required to reduce the risk to an acceptable level. Where there are many controls to be created then the risk analysis should prioritise the controls so that the greatest risks are mitigated first.

There are many risk analysis methods in use today. Some are highly complex creating a mathematical relationship and ranking involving asset values and probabilities. Many require detailed analysis of assets, threats, etc sometimes to the extent that reviewing the work is difficult. Many do not explicitly address the questions 'suppose the controls fail? What happens?'

We propose that business risks should be identified by first identifying undesirable events that could occur (e.g. loss of sales, fire, loss of IT functionality) and their consequent unwelcome impact(s) (e.g. failure of the business, unhappy customers, etc). Then deciding what is required to prevent the occurrence of the event, detect if an event has occurred and to minimise unwelcome impacts. The record of the decisions will be expressed in terms everyone can immediately relate to and identify with. Within such an analysis the level of detail can be set as that appropriate to the business.

Conclusion

All organisations need an Internal Control system. The best ICSs are those with high senior management involvement both in their creation and ongoing monitoring and high awareness by all the people involved in the business. To effectiveness of the Internal Control System is a combination of the ease with which people can understand the risk analysis and the monitoring of the time it takes to find and resolve incidents. The two factors together enable cost effective modifications to be made to the ICS in the light of the actual risks facing the organisation.