Risk analysis

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, August 2004.

Introduction

In our article published in the June Faculty Magazine we set out an overview of an Internal Control System (ICS), which in today's world is an essential part of the Corporate Governance system in all but the smallest organisations. ICSs should be developed using a risk analysis such as that recommended in the APB briefing paper 'Providing assurance on the effectiveness of internal control' published in July 2001. Often organisations 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.

Criteria for an effective methodology

An effective risk management methodology will enable:

- The senior management, as a whole
  - to understand the risks
  - together to participate in determining optimum countermeasures to risk
  - to allocate the overall 'control' spend to various risks across the whole business

- All staff concerned with design, implementation or performance of controls
  - to understand why the control is necessary
  - to determine when an implementation of a control fails to meet its objective, in whole or in part
  - to understand how failures in a control are detected

- Prompt revisions to be undertaken as circumstances change or incidents occur.

Depending on the complexity of the organisation and/or its technical infrastructure the whole risk management methodology may exist in tiers with varying levels of detail at each tier.

A pragmatic methodology

This methodology records the risks and their appropriate countermeasures in the form of a stylised story, which can be written by board members and understood by all employees.

To create these stories we first identify the major concerns of the senior management and we describe these as ‘events’. These would include failure of products, loss of customers, fire, loss of IT functionality, death of a key executive, etc. We then identify a number of impacts that any of these ‘events’ may lead to, for example, loss of revenue, unhappy customers, adverse press comment, a fall in the share price, etc.

Then for each of the identified ‘events’ the answers to the following questions are written down:

- Can the organisation prevent the ‘event’ from happening?
- Can the organisation detect when the event has happened, even if prevention measures are in place?
- Can the organisation minimise each of the adverse impacts, which would flow from the ‘event’ occurring?

In the course of answering the questions the organisation will identify and consider

- the assets at risk
- the threats to the organisation
- the vulnerabilities to which the organisation is exposed
- the probability of a particular event (or attack method) occurring
- the likely costs of particular controls.

In conducting any risk analysis it is probable that all major ‘events’, most of the major impacts and the obvious ways in which an event could materialise will be identified. These will constitute the applicable risks as defined in the APB briefing paper ‘Providing assurance on the effectiveness of internal control’ published in July 2001. It is unlikely that all the ways that would cause an ‘event’ to materialise will be identified. It is therefore essential to record what would happen if an event occurred irrespective of the reason why it occurred. This is the catch all of ‘unknown’ ways!

For each ‘event’ there will come a point where the residual exposure is acceptable to the organisation and this should be the end of the story.

Where there is substantial complexity the pragmatic results can be supplemented by more detailed risk analysis to determine how to meet the control objectives determined originally.

Conclusion

Risk analysis is a necessary part of determining the extent of the controls in an ICS. The pragmatic method of documenting the results of this work bring substantial benefits to the board and all employees.