

How is effectiveness measured in internal control systems?

By *William 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, October 2004.

Background

In previous articles we have discussed the effectiveness of internal control systems ([Chartec July](#)) and proposed a methodology for documenting a risk treatment plan ([Chartec Aug](#)). In this article we consider how to measure the real effectiveness of an internal control system.

There are many measurement systems and statistics in use. Most of these either

- measure the progress to an agreed plan of implementation of controls (or some performance metric) or
- measure the volume (and sometimes cost) of ‘incidents’ that occur or potential incidents avoided (e.g. the number of viruses trapped by the antivirus software or attacks detected by the IDS).

All these statistics are valuable but do not necessarily measure the effectiveness of the system under the management’s control. Those of the first kind measure performance against a plan but not whether the plan is any good. Those of the second kind measure the volume of threats to which the system is exposed at any one time, but not, for example, whether the internal control system will be effective in dealing with some new threat.

A different measure - time

The objective in the control part of the internal control system is to detect and rectify occurrences before they cause a material impact on the organisation. Following a risk assessment the organisation will have decided what controls it needs to address the identified risks the business faces. The management needs to know if the controls implemented are sufficient therefore it needs a measurement of the conduct of the system irrespective of the threats it faces. We propose that this measurement is time – how long does it take to detect an incident and how long does it take to rectify it.

To implement this measure there needs to be a complete record of incidents which record inter alia the nature of the incident, the actions taken and the two time measures. Yes we do appreciate that getting a complete record may be difficult as staff may not recognise an incident and may be reluctant to report their mistakes. However, the measure can also be used in designing the internal control system and that will give us a handle on whether the planned controls will be effective.

The record can then be analysed by type of incident (or cause of incident) and the average time for detection and rectification established.

In the light of the time metrics the following questions can be answered and action taken:

- Do the time metrics accord with expectations; if so, great - no further action required
- If it is taking too long to detect then:
 - For volumes of incidents additional preventive controls may be required or the control may need to be moved to another place in the overall system, or the implementation of the control requires modification because it is not achieving the objectives set for it
 - For isolated incidents consideration needs to be given to whether it is worth it to implement further controls (or even rectify faults in the system). In other words, these may constitute an acceptable risk.
- If the absolute volume of detected incidents causes delay in rectification: then additional preventive controls are required or the current controls require modification
- Are there individual incidents which cause material problems?

Some cautionary words

In complex systems the following may happen:

- A number of controls detect the same error ; there is then a danger of multiple rectification of the error causing further error
- It may not be possible to isolate the cause in complex IT systems
- In IT system there is often a custom of fixing all identified problems; this may be a misdeployment of resource if the effect of an incident does not warrant the cost of fixing it

- Software and hardware suppliers issue ‘fixes’ and upgrades to their offerings from time to time. Implementing these may cause incidents to occur and sometimes old incidents to recur.
- There is a risk that over time the result changes to the system, fault rectification etc that there will be too many controls in a system. Some redundant, some duplicating others, etc. Using the time metric system it is possible to remove controls selectively and very closely monitor the effect across the whole system.

Conclusion

Management need an effective measure of how effective their system is. The measure that is independent of the vagaries of the world is time. Monitoring the time taken to detect incidents and fix them measures the effectiveness of the system.