NOTICEBORED

Management briefing on

# IT audit metrics

**"A few well-chosen metrics can be a huge help in monitoring controls and measuring their effectiveness"**

*Clint Kreitner, SANS*

## Summary

This briefing outlines potential metrics for measuring and improving IT audit* (the topic of this month's security awareness materials), and is intended to stimulate discussion at management level.

## Introduction

IT audit's primary aim is to change the organization for the better by:

- Reviewing various aspects of the organization's use of IT systems, communications networks and data;
- Identifying, characterizing and pointing out to management, flaws/risks/inefficiencies in, or other opportunities to improve, the use of IT;
- Suggesting how things might be improved, discussing recommendations with management and gaining their commitment to address the identified issues in a reasonable timescale.

IT audits that do not lead to actual improvements are clearly failures while those that achieve dramatic improvements are clearly successful. The metrics in this briefing suggest how to measure audits in the middle ground, identifying their positions on the spectrum between failure and success and thereby providing a mechanism for management to get better value from IT audit. Furthermore, IT audit metrics need to take account of audit coverage, particularly in respect of whether auditors are truly reviewing high-risk or high-potential gain aspects of the organization.

## IT audit targets

Expanding on the previous paragraph, the central purpose of IT audit is to improve the organization's use of IT, reducing the associated risks and inefficiencies and increasing its effectiveness. It is not realistic for this generic briefing to suggest specific targets although we would encourage you to specify something along the lines of "Helping the organization increase the net benefit of IT by X% per annum".

* In fact, the same or very similar metrics should also work for non-IT audits.

# IT audit metrics

## Financial value metrics

Targeting increases in the net value of IT naturally implies measuring and accumulating IT-related cost reductions and benefit improvements that can be ascribed to IT audit work. Some values will be quite simple to measure (*e.g.* if IT audit work leads directly to a refund against a third party IT service level agreement or obvious savings on IT expenses) but most can only be estimated (as in "Without IT audit's involvement, we estimate that this IT project would have cost at least $Xm and achieved negligible benefits"). It is easy to get hung-up on the values, particularly estimates, and spend inordinate amounts of time discussing/arguing and refining the numbers. Remember that the purpose of these metrics is to drive out more value, not to get perfect numbers. Instead we recommend that the Head of Audit should maintain a simple spreadsheet listing his/her assessment of the values to be totaled, reported and discussed with the Audit Committee annually.

## Risk metrics

Measuring risk reductions is another area where estimation rules. Again, we suggest leaving the assessment to the Head of Audit. The annual report to the Audit Committee can usefully contain examples to illustrate IT risks that have been identified and addresses as a result of IT audit work.

## Work rate

IT audit, like any business function, can be measured in terms of the number of man-days expended, the salary and related costs (*e.g.* training), the number of audits completed *etc*. Such numbers are easy to obtain but unfortunately, in reality, they say little about the effectiveness of the function.

A better measure, we suggest, is to track 'IT audit plan coverage' *i.e.* the number of planned IT audits duly completed to an adequate quality standard during the year. Most if not all audit departments are resource-constrained – there is always more audit work that could have been done. The level of audit resourcing is often determined arbitrarily by management according to their anticipation of which audits are to be performed and the number of man-days each one will consume. One slight complication is to allow for un-preplanned work and "special investigations" that arise during the year – this is usually handled through contingency levels and preferred but optional audits.

## Confidence metrics

Management's confidence and trust in IT audit work is an important element of its success. It can be surveyed through questions such as this:

How confident are you that IT audits meet the business needs? Please mark the following percentage scale at the appropriate point, in your opinion.

0% 50% 100%

|----------+----------|

Not at all. Not quite enough | Just about enough Absolutely!

**Comments** *e.g.* what led you to this score? Have there been particular situations or incidents that influenced your decision?

It is a simple matter to measure percentage values from each response and calculate the mean score. Provided enough survey forms are completed (ideally more than 30), the results should be statistically valid. The comments can provide useful feedback and quotations for use in management reports and other awareness materials.

### Reporting

As noted earlier, the Head of Audit typically prepares an annual report to the Audit Committee. Additional quarterly or half-yearly progress reports to senior management may help adjust management's expectations around IT audit and, in particular, serve as opportunities to discuss current and recently completed audits.

## Conclusion

The suggested metrics are intended to help you derive creative and useful measures for your own situation. Do not underestimate the value of presenting and discussing metrics with management. The dialogue can be very effective at teasing out any underlying issues and concerns on both sides, and it promotes adequate investment in information security.

## For more information

Please visit Information Security's intranet Security Zone for further information. Additional security awareness materials and advice on this topic are available from the Information Security Manager. Professional bodies such as ISACA and the Institute of Internal Audit have further information on this topic.