

NOTICEBORED

We're from audit and we're here to help ...

Issue 59

IT Audit

April 2008

Editorial

Successful projects don't just happen — they are made to happen

Neal Whitten

IT auditors and information security professionals share a common interest in information security risk identification and management but from different perspectives. While security managers have the day-to-day hands-on responsibilities, auditors are hands-off and purely advisory. IT auditors are also concerned with other elements of IT governance, including governance of "IT projects". To be more accurate, these should perhaps be called "business improvement investments involving IT", which is the approach taken by an exciting new IT audit method from ISACA called [VallIT](#).

VallIT provides a sound conceptual framework for exploring the costs and benefits of IT development work, and tools for the business to maximize the realization of value. John Thorp, the father of VallIT, regrets that IT is even part of the name: "It's about the business, not IT!" he says. [John's groundbreaking 1999 book *The Information Paradox* retains a cherished spot on my bookshelf and is recommended reading for business managers struggling with IT demons.]

Since IT auditing is not a mainstream information security topic, NoticeBored last covered it more than three years ago. Aside from VallIT, maybe, IT audit is in much the same state as it was back then but NoticeBored has moved on, hence the updated module (all 38Mb of rich content!) is almost entirely new. ■

Gary Hinson, Editor

Background

"We're the auditors and we're here to help" may strike fear into some but through this month's security awareness materials we hope to dispel a few myths about IT auditors. Few people have had the pleasure* of being audited so we start with a basic introduction to auditing before moving on to the specifics of computer auditing.

The audit profession was once known for "tick and bash" straight compliance auditing. Thankfully, this has gradually been supplemented by more progressive audit methods involving greater cooperation and mutual respect between audit and management, although SOX auditors have a hard time.

More than ever before, auditors are focusing on the computer systems and telecommunications networks that drive their clients and underpin almost all business processes.

At the same time, however, the regulatory and legal penalties for inept audit work have increased, largely as a result of incidents such as Enron and Barings Bank. In both cases, it is recognized that information about the true status of the organizations concerned was available and should have been uncovered by the auditors.

About auditing

IT auditing is a branch of general auditing concerned with governance (management, security and control) of information and communications technologies.

Auditing largely involves "the *independent examination of records and other information* in order to form an opinion on the *integrity* of a system of controls and recommend control

* *Can you tell I used to be an IT auditor?*

improvements to limit risks". Auditors have to be independent *i.e.* not directly involved with the operations or management of a function or system being audited. They report to a separate line of management in order to be able to state the facts of a situation and their honest opinions without fear of recrimination from those working in the subject area. Independence is also a state of mind *i.e.* freethinking, able to consider situations objectively.

It is this independence of thought which creates audit's unique value

Records and other information includes what are often called "audit records" – in fact they are truly business records with value to business staff and managers, not just auditors. Auditors need to refer to information regarding the business processes and systems under review (such as completed data-entry forms, system-generated reports and, of course, the people involved in doing or managing the relevant business processes). IT auditors often use data analysis tools to examine computerized records. Furthermore, auditors normally interview staff in the business areas under review and may use other observational techniques to examine business processes in action.

**Audio-, aud-, audi-, audit- (Latin):
hearing, listening, perception
of sounds**

Lexfiles.com

Auditors gather and assess factual information from various sources – they do a lot of listening, watching and 'show me'. The formal outputs of the auditing process (primarily audit reports containing recommendations for control improvements) must be traceable to valid information sources, in other words facts.

Fact-based assessment adds another string to audit's powerful bow

Auditors provide both objective facts and subjective opinions on a given situation. Although subjective, their opinions are based on an interpretation of the facts and are open to legitimate challenge. What's more, auditors often challenge the *status quo*.

Objective challenge to accepted practices is yet another important benefit of auditing

Integrity literally means completeness, accuracy and trustworthiness. A control system which is only partially effective may be better than nothing, or it may give a false sense of security: either way, the auditor will probably not be impressed. [We will be covering integrity, trust and related matters in much more depth next month's security awareness topic.]

“Getting an auditor to revise an assessment does not require a "strategy": just facts. An auditor's function is to provide an independent and objective opinion on the activity, project, subject, etc, that's "under review." If you can provide facts that support your viewpoint, the auditors should adjust their opinion. If you can't provide the facts, you cannot expect the auditors to change the report. Disagreements are generally painful—awkward at best, disastrous at worst. Thus, you should have two goals whenever you disagree with your auditor: (1) resolving the disagreement, and (2) figuring out how to prevent disagreements in future audit cycles.”

Dan Swanson, IT Compliance Institute Q&A

Systems of controls operate at many levels. Experienced IT auditors are specialists in control, competent to examine technical controls built-in to the IT systems, of course, but also procedural controls (IT operations procedures, IT process management *etc.*), legal and regulatory controls, personnel controls (policies, employment contracts *etc.*), physical controls and so on.

Auditors generate "recommendations" which are just that – more than mere suggestions but not mandatory obligations. Auditors don't have the authority to implement recommendations themselves, nor can they force management to do so. Improvements in the organization are achieved mostly by a process of explanation, justification and persuasion, explaining the risks represented by control weaknesses, justifying the need to change systems and/or processes, and persuading management to apply the necessary resources and direction in order to address the risks. At the end of the day, managers, not auditors, carry the can and remain accountable for their decisions. Mind you, auditors do have the ear of senior managers and other influential stakeholders.

Ignore the auditors at your peril!

Improving the system of controls generally means adding additional controls. In rare cases, however, auditors may recommend deprecating or removing controls that are ineffective, disruptive or wasteful.

Risks, like fraudulent politicians or spam emails, can be reduced but not totally eliminated. Good business involves minimizing risks cost-effectively, and being prepared for the worst if things go wrong (contingency planning). Risk is the chance combination of threats (usually caused by someone with malicious intent, sometimes just due to carelessness or incompetence), acting on vulnerabilities (weaknesses in 'the system', typically due to a lack of controls in many computer systems and operating procedures) to cause impacts (adverse outcomes *i.e.* financial, human and political fallout when it all goes horribly wrong).

Internal vs. external audit

Whereas external auditors are employed and assigned by audit companies, internal auditors are normally employees of the organization being audited. This is the most obvious difference between them but there are further albeit more subtle differences in attitude and working practices reflecting different purposes.

Formal external audits such as SOX audits are usually mandated by law on corporations and public bodies, in other words they are externally initiated and controlled. The external auditors are paid to form and state an independent opinion on the client's governance and control systems, and to review the company accounts to determine whether they form a full and accurate picture of the organization's affairs. As [Arthur Anderson LLP](#) discovered to their cost in the Enron debacle, external auditors are legally obliged to take all reasonable steps to verify the facts supporting their assertions.

Internal audits, by contrast, are initiated and controlled by management for internal management purposes, in much the same way that management accountants are more concerned with effective operational control of the organization's finances than in the external reporting issues beloved of their financial accounting colleagues. Whilst this could be seen as a drawback, greater access to management information can make internal

audit more effective than external audit in many situations.

In practice, active cooperation between internal and external auditors, plus other governance, risk and security specialists, gives the best of all worlds, provided as always that it doesn't cross the line of independence.

IT auditing *versus* accounting

The audit profession arose out of accounting but has evolved substantially. An IT auditor might be asked to review certain aspects of accounting within the IT department (e.g. financial management of IT projects, budgeting or forecasting) but that kind of assignment is more likely to be performed by a conventional internal/external auditor or accountant with a recognized accountancy qualification. The study of an organization's financial/management accounting system would typically be done by an IT auditor (checking the technical design and operation of the system) and/or an accountant (checking that the system was being used correctly, accounting rules were being followed *etc.*): the most effective audits on accounting systems employ auditors with both IT audit and accounting qualifications, or teams containing both types of auditor.

“The benefits of computer audit are: business efficiency; security; standardization; asset tracking; asset replacement policy; accounting; cost control; and competitive advantage.”

Extract from a piece by [Small Business Resource](#).

Compliance auditing

Many audits include an element of testing compliance against internally-generated corporate policies/standards/procedures or externally-imposed laws, regulations and contractual terms ... but the bulk of compliance activities fall to management not audit. Other than a high-level assessment, the auditors are more likely to check whether management processes for achieving compliance are effective, and that “the rules” are suitable and sufficient, and so on, than to assess the extent of compliance in detail. That said, managers who fail in their compliance responsibilities are likely to be criticized if the auditors uncover

excessive and obvious examples of noncompliance.

Relationships between IT auditing, IT governance, IT risk management and information security management

Governance can be considered at various levels such as broad pan-organizational controls (corporate governance) or controls over individual projects or systems (project and systems governance). Similarly in respect of risk management, the scope can apply across the whole organization (taking in commercial, operational, market, financial, regulatory and other risks) or just specific projects and systems. Auditors have a professional interest in governance, risk and security management throughout the organization.

Specifically in relation to IT, proactive management of IT risks implies the design, implementation, operation, management and maintenance of appropriate technical, procedural and physical controls. IT auditors are concerned with the effective management IT risks and therefore are interested in information security controls. They also have an interest in higher-level management controls to ensure, for instance, that the entire security controls framework (the Information Security Management System in modern parlance) is properly directed and funded, and that the IT function is structured and controlled to make the best use of available funds.

Information security managers develop, implement and operate information security control systems to enhance IT governance and contribute to corporate governance. This clearly includes an operational day-to-day hands-on function. IT auditors review IT governance/control systems in order to ascertain whether risks (including information security risks) are minimized. These may sound similar but are fundamentally different rôles: information security managers have executive responsibilities for securing the organization's information assets against hackers, malware and other threats. Auditors occasionally review,

advise, report and persuade. The common ground is cost-effective minimization of risks.

Whilst that may be reasonably straightforward in theory, there is a lot of confusion about the terms in practice. The term 'governance', for instance, is often used as shorthand for 'corporate governance'. IT controls may be an important part of corporate governance, especially in organizations that are critically reliant on information processing, but there are many other types of control in most organizations that fall well outside the scope of IT (e.g. the use of non-executive directors to review and guide executive management has nothing to do with IT). Experienced and qualified IT auditors have a solid understanding of the practicalities of implementing their recommendations, yet if necessary are able to persuade management to go well beyond their comfort zones.

COBIT supports IT governance by providing a framework to ensure that:

- IT is aligned with the business
- IT enables the business and maximizes benefits
- IT resources are used responsibly
- IT risks are managed appropriately

Implementing COBIT allows for:

- Better alignment based upon a business focus
- An understandable view of IT for management
- Clear ownership and responsibilities
- General acceptability with third parties and regulators
- Shared understanding among all stakeholders based on a common language
- Fulfillment of the COSO requirements












[*COBIT 4.1 brochure*](#) from ISACA

Conclusion



The newsletter has rambled through an overview of some of the defining characteristics and activities that IT auditors perform. There's plenty more meat on the bones in the security awareness materials provided to customers this month: others will have to settle for the online [IT Audit FAQ](#), I'm afraid. ■


April's NoticeBored Classic awareness module


Awareness materials for all employees


1. **Awareness seminar: IT audit**  14 slides
Relatively few people are lucky enough to have had direct contact with IT auditors. The seminar is the next best thing.
2. **Awareness poster images: IT audit**  x12
Six brand new high-resolution poster images plus six environmentally-friendly recycled ones.
3. **Screensavers: IT audit**  x4
Reinforce key awareness messages daily.
4. **Guideline: IT auditing**  2 pages
Leaflet/desk-drop offers general advice to staff on IT audit issues they are likely to encounter.
5. **Case studies: IT audit**  x2, 2 pages each
Two IT audit-related scenarios to explore and discuss in a class setting.
6. **Take home messages: IT audit**  1 page
Summarizes the entire awareness module.
7. **Crossword puzzle: IT audit**  with answers!
8. **Security awareness survey form**  1 page
9. **Security awareness test: IT audit**  1 page
How well do staff comprehend and recall the information in this awareness module?
10. **Glossary: IT audit terms**  3 pages
3 side glossary with hyperlinked explanations.
11. **Links: IT audit resources** 
Annotated hyperlinks to [IT audit resources](#) on the Web.

Awareness materials for managers


12. **Mind-maps: IT audit**  x6
Pictorial representations of the topic.
13. **Board agenda: IT audit**  1 page
We're experimenting with a slight change to the format this month: one of the usual sliding scale questions is now a multiple-choice.

14. **Model security policy: IT audit**  4 pages
2 high-level axioms (such as default read-only permission for IT auditors to corporate information) plus 9 specific policy requirements.


15. **Policy: audit & security logging**  3 pages
Requirements for specification and secure configuration of audit and system security logs.

16. **Management seminar: IT audit**  11 slides
Lays out the full scope and value of IT audit work. Find out how IT auditors can help you.

17. **Executive briefing: IT audit**  1 page

18. **Mgmt briefing: IT audit**  2½ pages


A little more info to accompany the seminar.


19. **Mgmt brief: IT auditor interview checklist**  2 pages of questions to ask auditor candidates.


20. **Metrics: IT audit**  2½ pages


Track IT audit's work to maximize the value.


Awareness materials for IT pro's


21. **This newsletter: IT audit**  6 pages
Introduces the topic and explores the key risks.


22. **Awareness activities: IT audit**  5½ pages
Topic-related hints to those responsible for managing and delivering security awareness on making the program more effective.

23. **Tech seminar: IT project audits**  13 slides
Explains the yin and yang of project auditing.

24. **Technical briefing: IT audit**  4½ pages
Describes audit processes & working methods.

25. **Tech guide: IT project auditing**  21 pages
Explains the value of auditing IT developments from cradle-to-grave, including system security.

26. **White paper : IT audit FAQ**  44 pages
For several years, IsecT has published and maintained on the web our "Frequently Avoided Questions on IT audit" as a PDF. Latest update.

27. **Review checklist: IT audit**  6 pages
How well is your IT audit function doing? Audit the IT auditors with our checklist. ■

NoticeBored topic diary

We are currently researching and preparing awareness materials on the topics listed below. To contribute to these modules or propose other topics, please email info@NoticeBored.com.

May – fraud, integrity and trust

Identity thefts, 419 scams, pump-n-dumps, Ponzi/pyramid schemes, deliberate sabotage by trusted insiders and numerous other information security incidents provide no shortage of topical material for our next module. Technological controls alone are seldom adequate to reduce the risks, placing emphasis on human controls through training and education, policies and procedures, and various forms of management supervision (including, by the way, IT audits).

June – passwords, login IDs and phishing (core awareness topic)

Persuading computer users to choose strong passwords and keep them private remains an important information security control since passwords are still the most widely used method of authenticating people to IT systems and networks. Decades of experience have taught us about password pitfalls so we'll be sharing some simple passwords tips to help protect you, your peers, family and friends from identity theft.

July – information security and risk management

This module will give a peek into the methods used to examine and manage information security risks and controls. Find out why many greybeard security professionals are finally admitting that the risk analysis methods we have promoted for years are little better than chicken entrails at predicting the future. ■

NoticeBored news

Over at www.ISO27001security.com, we recently published the latest product of a collaborative effort by members of the ISO27k Implementers' Forum – an ISMS auditing guideline. It's our joint contribution to the development of the draft ISO/IEC 27007 standard on ISMS auditing. There's also a new sample security policy on outsourcing IT and various other generic example documents and guidelines are downloadable from the site. If you are working towards compliance with ISO/IEC 27001, we hope they will prove useful.

We have a tongue-in-cheek offer this month for those of you who keep pestering us to buy our [posters](#) – just our posters. Thus far we have steadfastly refused to sell the posters in isolation because, in our opinion, they will not achieve much awareness of information security issues. The short text messages and eye-catching graphics are designed to do just that - catch people's eyes, perhaps raise a curious smile and hopefully spark an interest in the monthly topic. The remaining awareness materials explain things in full but the posters alone don't make much sense without the rest of the module as context.

So, here's the offer. We will happily sell you the posters at the same [very reasonable price](#) that we charge for NoticeBored Classic ... and we'll throw in the accompanying awareness materials for free ☺ ■



Newsletter published by:

[Isect Ltd.](#)
Dunard
536 Okirae Road
RD7 Wanganui
New Zealand

Tel: +64 634 22922

Copyright and disclaimer

All NoticeBored materials including this newsletter are protected by international copyright law. For more information, please contact the copyright holder, Isect Limited (visit www.isect.com or see above for our contact details).

You are encouraged to circulate the Adobe Acrobat PDF version of this newsletter to anyone *provided* that it remains unchanged and intact (including this copyright notice), is not embedded in any other product or service and is provided free of charge. The MS Word RTF version is provided to customers purely for internal use as per the NoticeBored license.

The information in this newsletter is provided free, for information only and 'as is'. Whilst believed correct, it is in no way comprehensive. It is provided for interest only and is not intended to be relied upon as formal advice. It is not legal advice. Seek your own legal advice from a qualified legal practitioner, not us. No liability is accepted for any errors or for any losses that may be incurred if any such information is relied upon.